EXHIBIT 1

Exhibit F

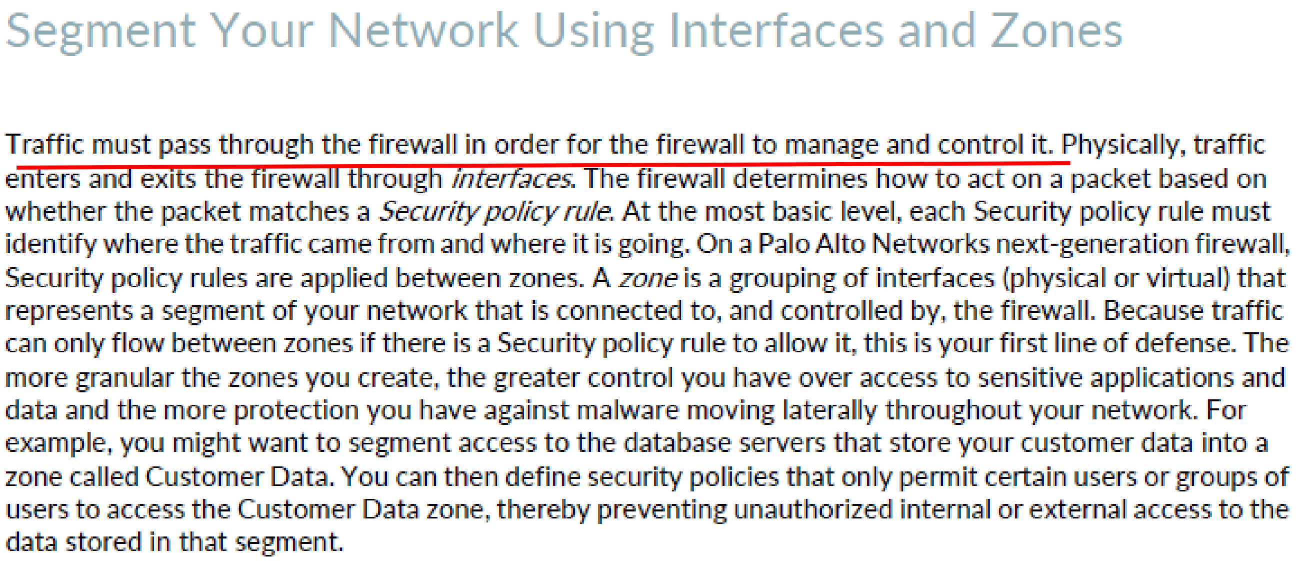
Claim Chart Demonstrating That PAN's Next-Generation Firewalls Infringe Claims 1-4, 10, 13, 16, 19 of U.S. Patent No. 9,591,104 (the "'104 patent")

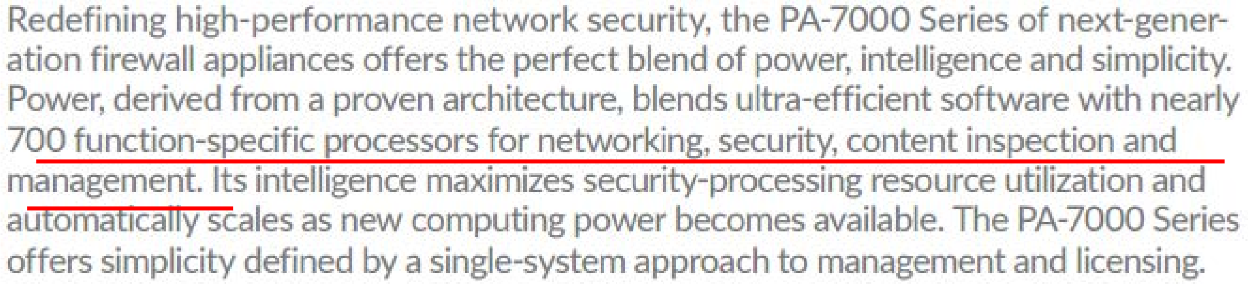
As shown below, Palo Alto Networks, Inc.'s ("PAN's") next-generation firewalls, including without limitation PA-7000, PA-5200, PA-5000, PA-3000, PA-800, PA-500, PA-220, PA-200, VM-700, VM-500, VM-300, VM-100, and VM-50 Series next-generation firewalls running PAN-OS 8.0, all substantially similar products, and all associated computer hardware, software and digital content (the "Accused System and Method") infringe claims 1-4, 10, 13, 16, 19 of the '104 Patent. By identifying exemplary evidence in this chart of where a limitation of an asserted claim may be found in the Accused System and Method, Plaintiff may address a range of potential claim constructions of such limitation, including constructions with which Plaintiff may disagree.

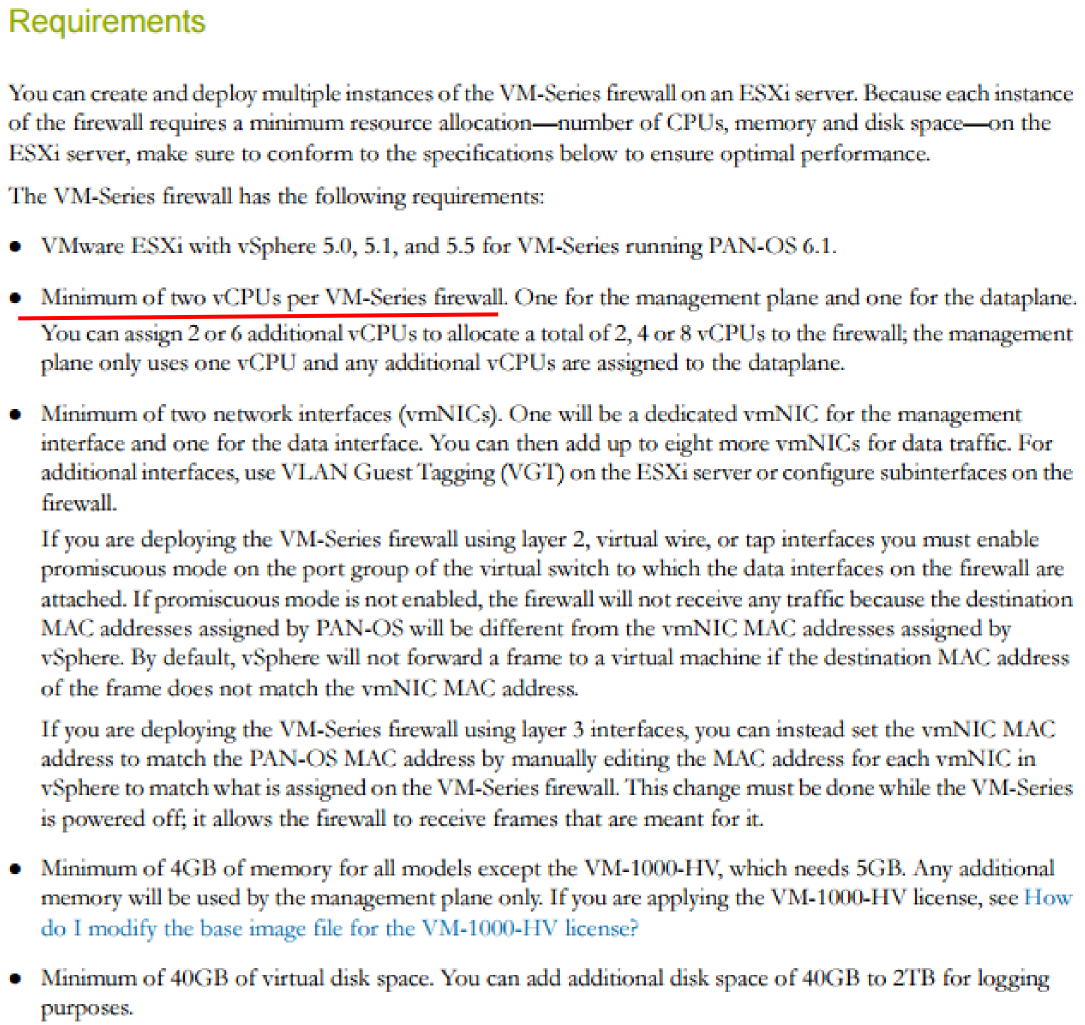
Plaintiff further accuses PAN of indirectly infringing the '104 Patent through providing, authorizing and instructing regarding the Accused System and Method to others, including its customers. Installing or activating the Accused System and Method and the operation thereof directly infringe the asserted claims. PAN intends to cause infringement by its customers and users. PAN instructs users to use the Accused System and Method in an infringing manner. PAN enacts contractual protections requiring that the Accused System and Method be used in a manner intended by PAN. PAN further instructs users to configure and operate the Accused System and Method in an infringing manner. PAN also provides support services for the Accused System and Method, including providing instructions, guides, online materials and technical support.

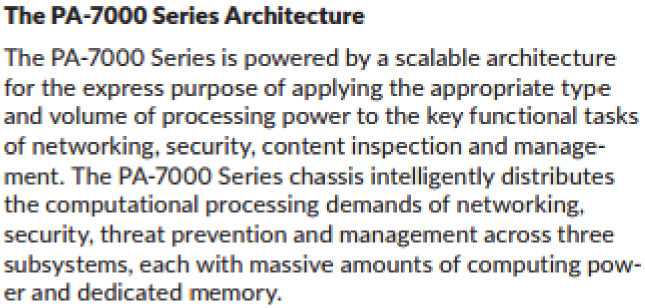
The asserted claims include elements that are implemented, at least in part, by proprietary electronics and software in the Accused System and Method. The precise designs, data structures, processes, and algorithms used in them are held secret, at least in part, and are not publicly available in their entirety. An analysis of PAN Micro's documentation and/or source code may be necessary to fully and accurately describe all infringing features and functionality of the Accused System and Method and, accordingly, Plaintiff reserves the right to supplement these contentions once such information is made available to Plaintiff, including for example pursuant to P.R. 3-1(g). Furthermore, Plaintiff reserves the right to revise these contentions, including as discovery in the case progresses, in view of the Court's final claim construction in this action and in connection with the provision of its expert reports. Plaintiff further reserves the right to supplement this chart to allege infringement under the doctrine of equivalents if it is found that the accused instrumentalities do not literally meet or practice a particular claim element for any of the claims.

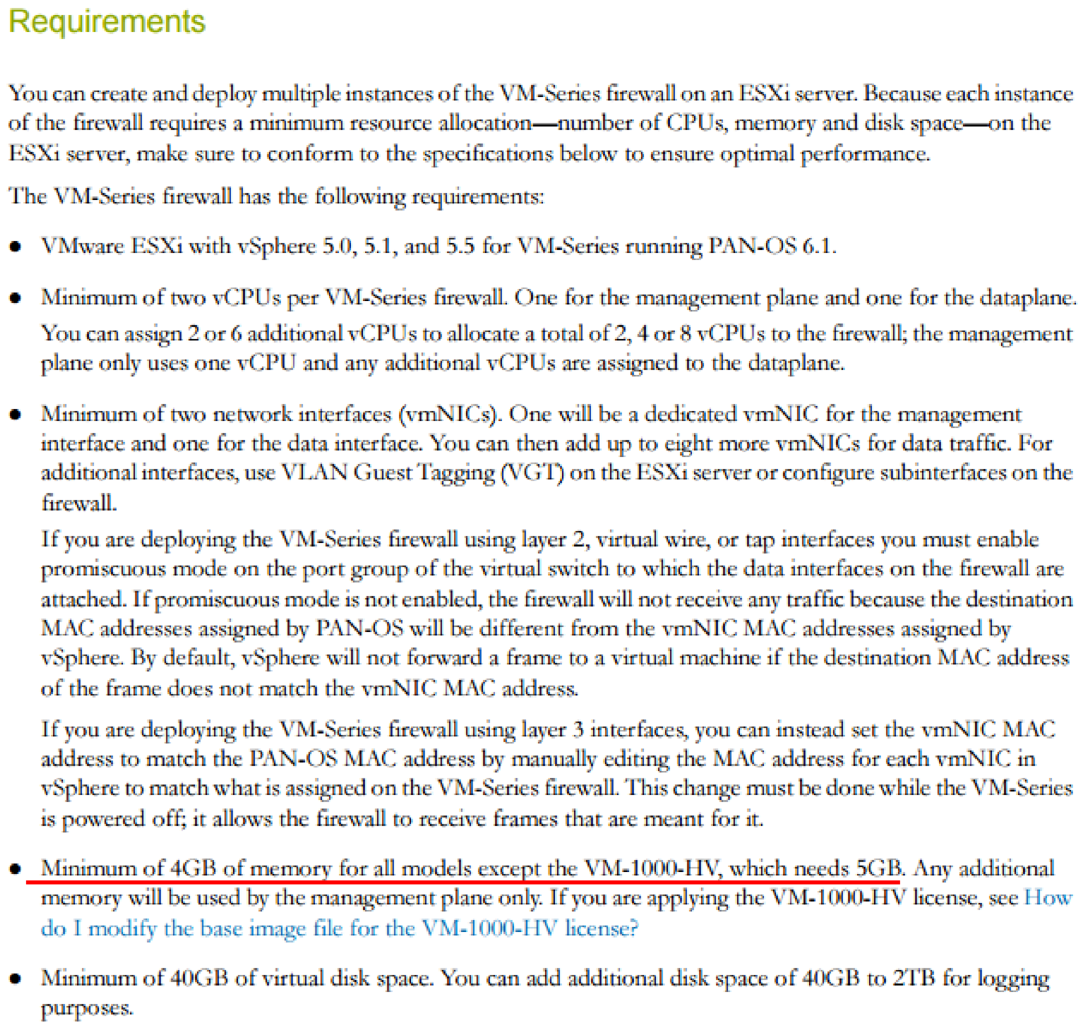
Exhibit F to Implicit's P.R. 3-1 Disclosures: Pre-Discovery, Pre-Claim Construction Claim Chart re PAN's Next-Generation Firewalls' Infringement of the '104 Patent

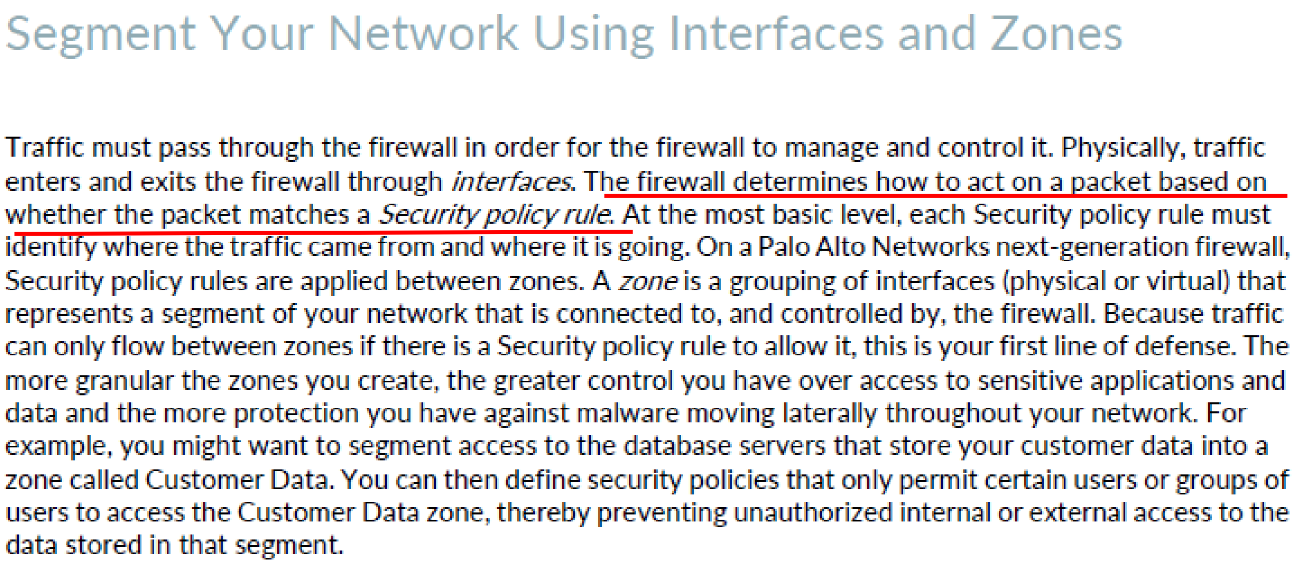
Claim 1	Exemplary Evidence of Infringement
1[A] An apparatus, comprising;	The Accused System and Method includes an apparatus, *e.g.*, PAN's firewalls and virtual firewalls running PAN-OS 8.0.  Segment Your Network Using Interfaces and Zones Traffic must pass through the firewall in order for the firewall to manage and control it. Physically, traffic enters and exits the firewall through *interfaces*. The firewall determines how to act on a packet based on whether the packet matches a *Security policy rule*. At the most basic level, each Security policy rule must identify where the traffic came from and where it is going. On a Palo Alto Networks next-generation firewall, Security policy rules are applied between zones. A *zone* is a grouping of interfaces (physical or virtual) that represents a segment of your network that is connected to, and controlled by, the firewall. Because traffic can only flow between zones if there is a Security policy rule to allow it, this is your first line of defense. The more granular the zones you create, the greater control you have over access to sensitive applications and data and the more protection you have against malware moving laterally throughout your network. For example, you might want to segment access to the database servers that store your customer data into a zone called Customer Data. You can then define security policies that only permit certain users or groups of users to access the Customer Data zone, thereby preventing unauthorized internal or external access to the data stored in that segment. **Source:** *PAN-OS Administrator's Guide, Pg. 36,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf
1[B] a processing unit; and	The Accused System and Method provides a processor in the apparatus. For example, PAN's 7000 series firewall units contain multiple processors.

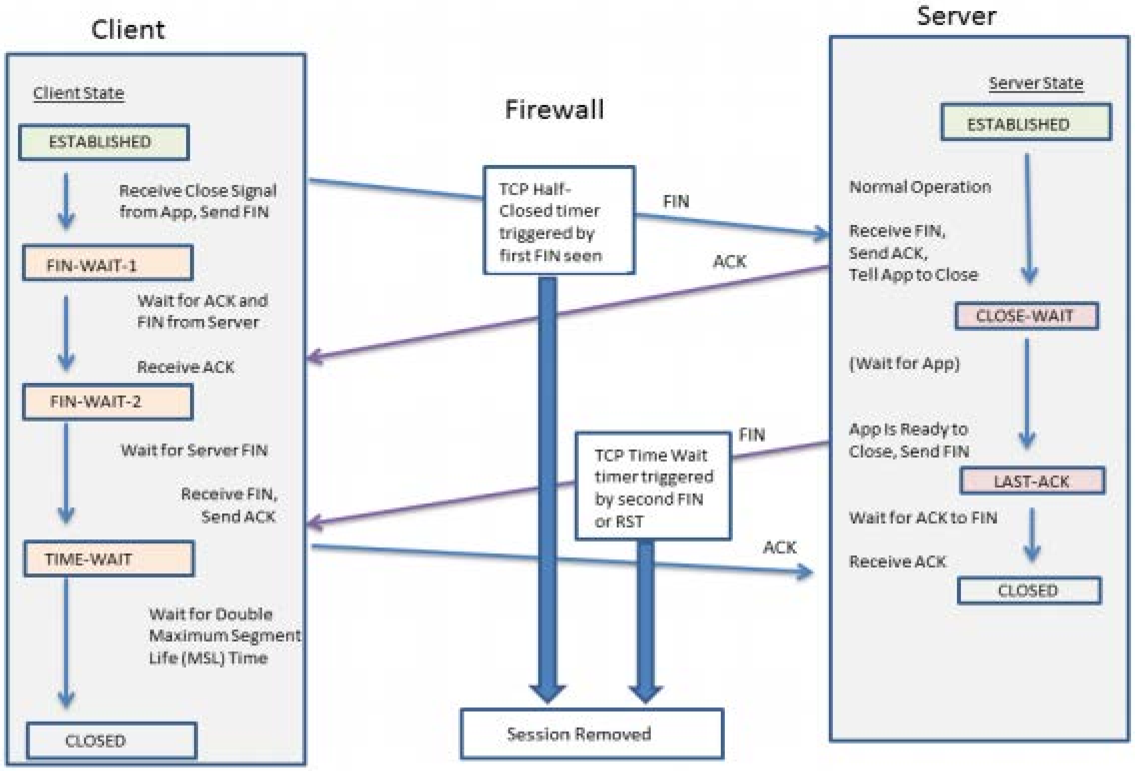
	 Redefining high-performance network security, the PA-7000 Series of next-generation firewall appliances offers the perfect blend of power, intelligence and simplicity. Power, derived from a proven architecture, blends ultra-efficient software with nearly 700 function-specific processors for networking, security, content inspection and management. Its intelligence maximizes security-processing resource utilization and automatically scales as new computing power becomes available. The PA-7000 Series offers simplicity defined by a single-system approach to management and licensing. **Source:** https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series

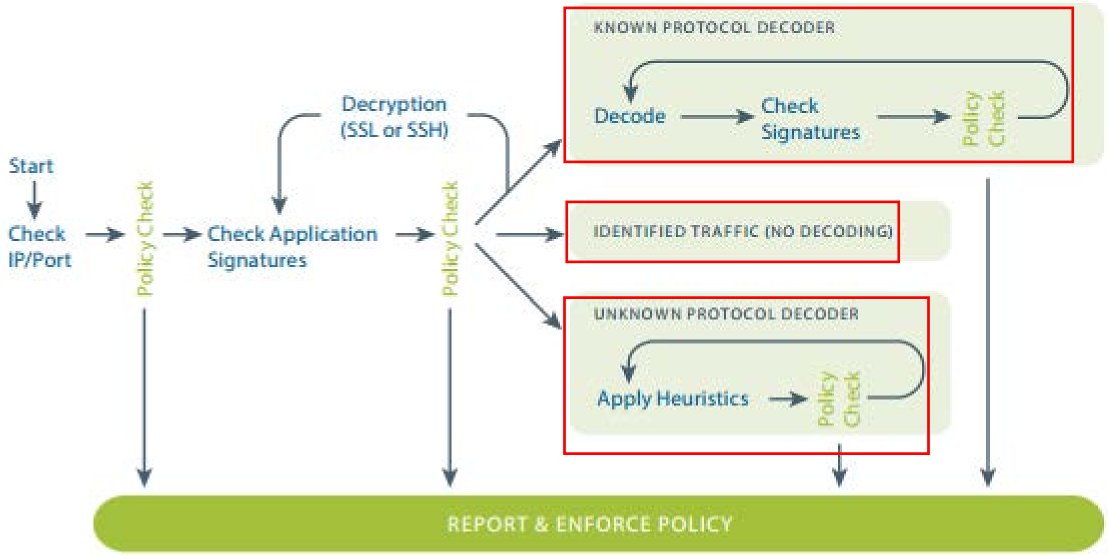
	 Requirements You can create and deploy multiple instances of the VM-Series firewall on an ESXi server. Because each instance of the firewall requires a minimum resource allocation—number of CPUs, memory and disk space—on the ESXi server, make sure to conform to the specifications below to ensure optimal performance. The VM-Series firewall has the following requirements: ● VMware ESXi with vSphere 5.0, 5.1, and 5.5 for VM-Series running PAN-OS 6.1. ● Minimum of two vCPUs per VM-Series firewall. One for the management plane and one for the dataplane. You can assign 2 or 6 additional vCPUs to allocate a total of 2, 4 or 8 vCPUs to the firewall; the management plane only uses one vCPU and any additional vCPUs are assigned to the dataplane. ● Minimum of two network interfaces (vmNICs). One will be a dedicated vmNIC for the management interface and one for the data interface. You can then add up to eight more vmNICs for data traffic. For additional interfaces, use VLAN Guest Tagging (VGT) on the ESXi server or configure subinterfaces on the firewall. If you are deploying the VM-Series firewall using layer 2, virtual wire, or tap interfaces you must enable promiscuous mode on the port group of the virtual switch to which the data interfaces on the firewall are attached. If promiscuous mode is not enabled, the firewall will not receive any traffic because the destination MAC addresses assigned by PAN-OS will be different from the vmNIC MAC addresses assigned by vSphere. By default, vSphere will not forward a frame to a virtual machine if the destination MAC address of the frame does not match the vmNIC MAC address. If you are deploying the VM-Series firewall using layer 3 interfaces, you can instead set the vmNIC MAC address to match the PAN-OS MAC address by manually editing the MAC address for each vmNIC in vSphere to match what is assigned on the VM-Series firewall. This change must be done while the VM-Series is powered off; it allows the firewall to receive frames that are meant for it. ● Minimum of 4GB of memory for all models except the VM-1000-HV, which needs 5GB. Any additional memory will be used by the management plane only. If you are applying the VM-1000-HV license, see How do I modify the base image file for the VM-1000-HV license? ● Minimum of 40GB of virtual disk space. You can add additional disk space of 40GB to 2TB for logging purposes. **Source:** https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/61/virtualization/Virtualization/section_2.pdf
1[C] a memory storing instructions executable	The Accused System and Method provides a memory that stores instructions executable by one or more processing units in the apparatus.

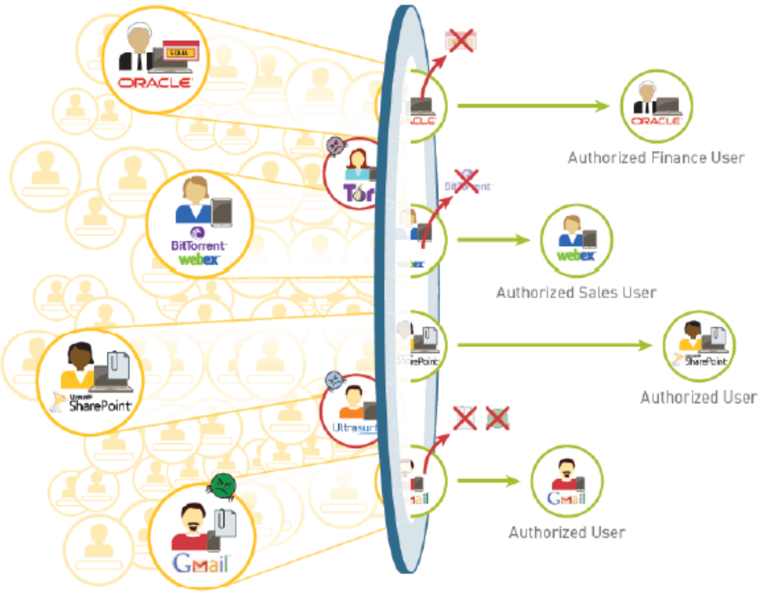
by the processing unit to:	 **The PA-7000 Series Architecture** The PA-7000 Series is powered by a scalable architecture for the express purpose of applying the appropriate type and volume of processing power to the key functional tasks of networking, security, content inspection and management. The PA-7000 Series chassis intelligently distributes the computational processing demands of networking, security, threat prevention and management across three subsystems, each with massive amounts of computing power and dedicated memory. **Source:** https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/datasheets/pa-7000-series

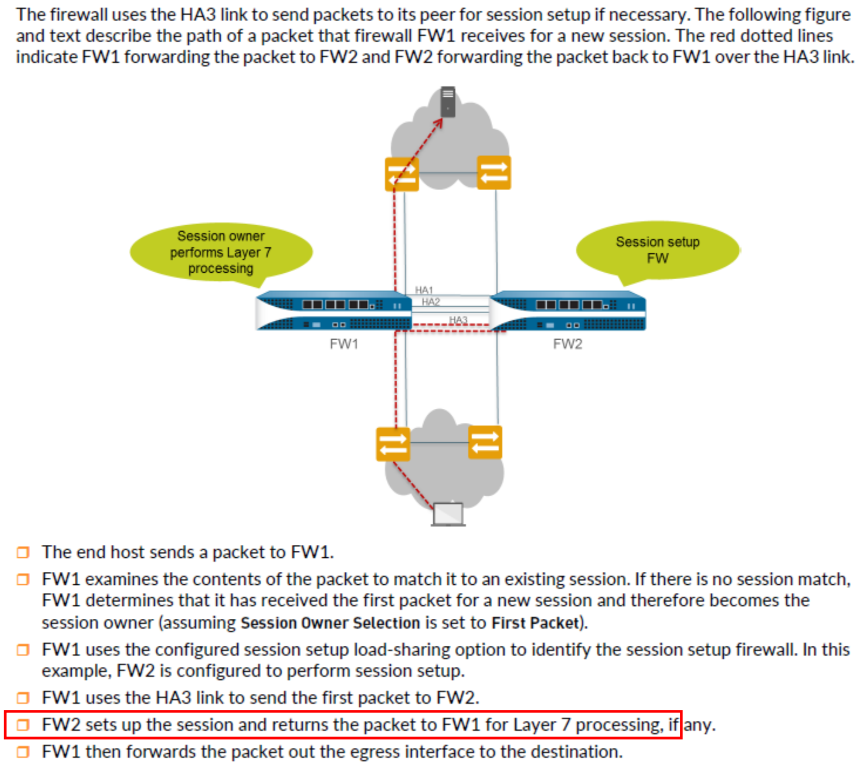
	 Requirements You can create and deploy multiple instances of the VM-Series firewall on an ESXi server. Because each instance of the firewall requires a minimum resource allocation—number of CPUs, memory and disk space—on the ESXi server, make sure to conform to the specifications below to ensure optimal performance. The VM-Series firewall has the following requirements: • VMware ESXi with vSphere 5.0, 5.1, and 5.5 for VM-Series running PAN-OS 6.1. • Minimum of two vCPUs per VM-Series firewall. One for the management plane and one for the dataplane. You can assign 2 or 6 additional vCPUs to allocate a total of 2, 4 or 8 vCPUs to the firewall; the management plane only uses one vCPU and any additional vCPUs are assigned to the dataplane. • Minimum of two network interfaces (vmNICs). One will be a dedicated vmNIC for the management interface and one for the data interface. You can then add up to eight more vmNICs for data traffic. For additional interfaces, use VLAN Guest Tagging (VGT) on the ESXi server or configure subinterfaces on the firewall. If you are deploying the VM-Series firewall using layer 2, virtual wire, or tap interfaces you must enable promiscuous mode on the port group of the virtual switch to which the data interfaces on the firewall are attached. If promiscuous mode is not enabled, the firewall will not receive any traffic because the destination MAC addresses assigned by PAN-OS will be different from the vmNIC MAC addresses assigned by vSphere. By default, vSphere will not forward a frame to a virtual machine if the destination MAC address of the frame does not match the vmNIC MAC address. If you are deploying the VM-Series firewall using layer 3 interfaces, you can instead set the vmNIC MAC address to match the PAN-OS MAC address by manually editing the MAC address for each vmNIC in vSphere to match what is assigned on the VM-Series firewall. This change must be done while the VM-Series is powered off; it allows the firewall to receive frames that are meant for it. • Minimum of 4GB of memory for all models except the VM-1000-HV, which needs 5GB. Any additional memory will be used by the management plane only. If you are applying the VM-1000-HV license, see How do I modify the base image file for the VM-1000-HV license? • Minimum of 40GB of virtual disk space. You can add additional disk space of 40GB to 2TB for logging purposes. **Source:** https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/61/virtualization/Virtualization/section_2.pdf
1[D] receive one or	The Accused System and Method is configured to receive packets of a message.

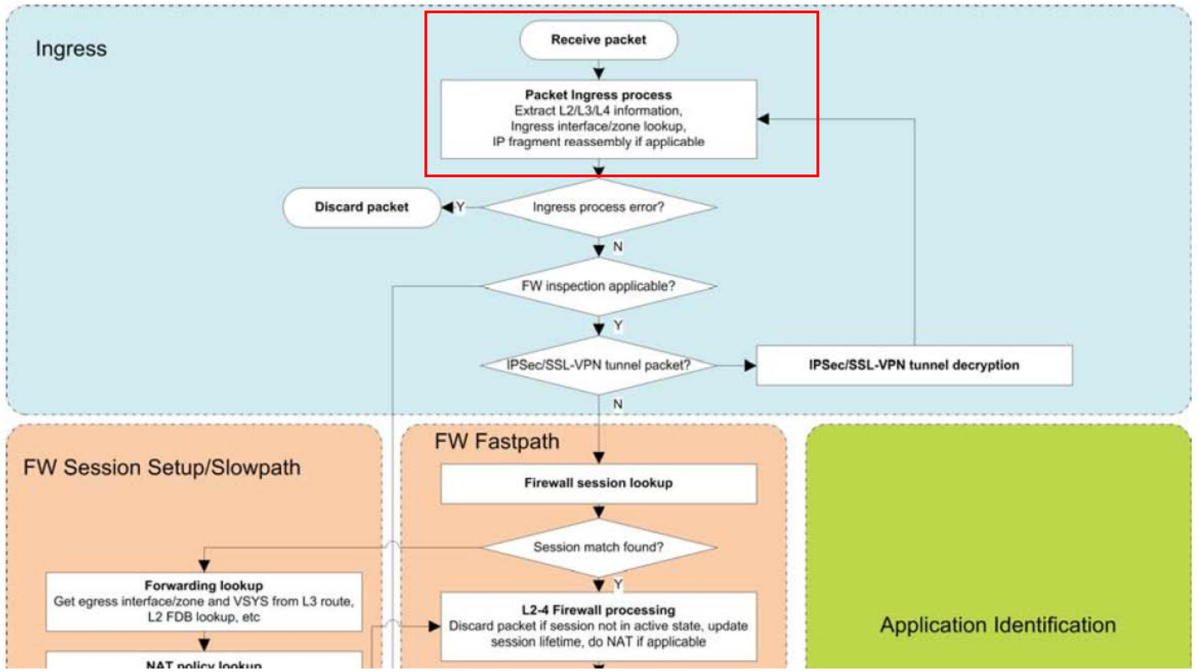
more packets of a message;	 Segment Your Network Using Interfaces and Zones Traffic must pass through the firewall in order for the firewall to manage and control it. Physically, traffic enters and exits the firewall through *interfaces*. The firewall determines how to act on a packet based on whether the packet matches a *Security policy rule*. At the most basic level, each Security policy rule must identify where the traffic came from and where it is going. On a Palo Alto Networks next-generation firewall, Security policy rules are applied between zones. A *zone* is a grouping of interfaces (physical or virtual) that represents a segment of your network that is connected to, and controlled by, the firewall. Because traffic can only flow between zones if there is a Security policy rule to allow it, this is your first line of defense. The more granular the zones you create, the greater control you have over access to sensitive applications and data and the more protection you have against malware moving laterally throughout your network. For example, you might want to segment access to the database servers that store your customer data into a zone called Customer Data. You can then define security policies that only permit certain users or groups of users to access the Customer Data zone, thereby preventing unauthorized internal or external access to the data stored in that segment. **Source:** *PAN-OS Administrator's Guide, Pg. 36*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

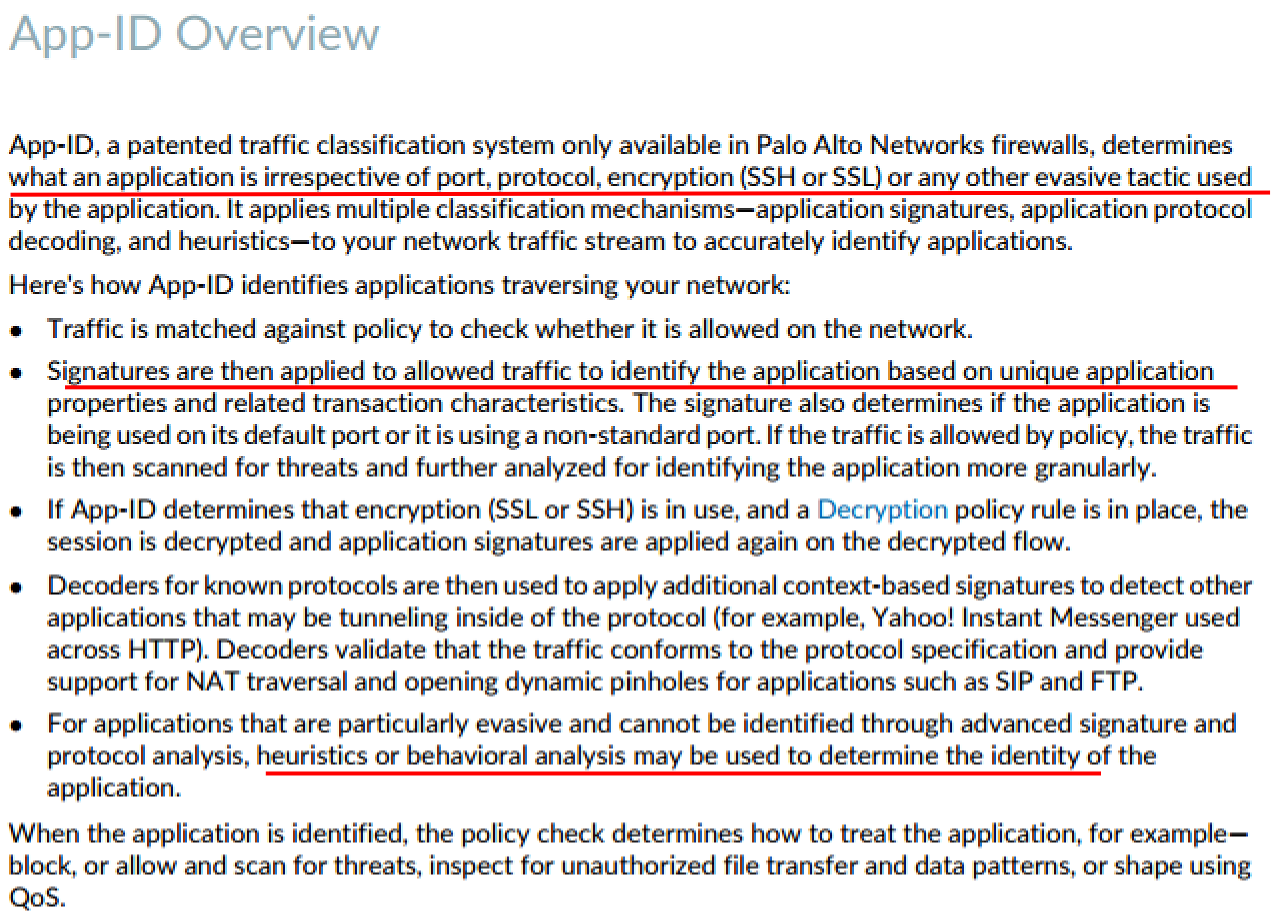
	 Client Client State ESTABLISHED Receive Close Signal from App, Send FIN FIN-WAIT-1 Wait for ACK and FIN from Server Receive ACK FIN-WAIT-2 Wait for Server FIN Receive FIN, Send ACK TIME-WAIT Wait for Double Maximum Segment Life (MSL) Time CLOSED Firewall TCP Half-Closed timer triggered by first FIN seen FIN ACK TCP Time Wait timer triggered by second FIN or RST FIN ACK Session Removed Server Server State ESTABLISHED Normal Operation Receive FIN, Send ACK, Tell App to Close CLOSE-WAIT (Wait for App) App Is Ready to Close, Send FIN LAST-ACK Wait for ACK to FIN Receive ACK CLOSED **Source:** *PAN-OS Administrator's Guide, Pg. 916*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 KNOWN PROTOCOL DECODER Decode Check Signatures Policy Check Decryption (SSL or SSH) Start Check IP/Port Policy Check Check Application Signatures Policy Check IDENTIFIED TRAFFIC (NO DECODING) UNKNOWN PROTOCOL DECODER Apply Heuristics Policy Check REPORT & ENFORCE POLICY **Figure 1:** How App-ID classifies traffic. *App-ID Tech Brief*, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/app-id-tech-brief

	 ORACLE Tor BitTorrent webex SharePoint UltraSurf Gmail Authorized Finance User Authorized Sales User Authorized User Authorized User The best practice policy is based on the following methodologies. The best practice methodologies ensure detection and prevention at multiple stages of the attack life cycle. **Source:** *PAN-OS Administrator's Guide, Pg. 963*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 The firewall uses the HA3 link to send packets to its peer for session setup if necessary. The following figure and text describe the path of a packet that firewall FW1 receives for a new session. The red dotted lines indicate FW1 forwarding the packet to FW2 and FW2 forwarding the packet back to FW1 over the HA3 link. Session owner performs Layer 7 processing Session setup FW HA1 HA2 HA3 FW1 FW2 □ The end host sends a packet to FW1. □ FW1 examines the contents of the packet to match it to an existing session. If there is no session match, FW1 determines that it has received the first packet for a new session and therefore becomes the session owner (assuming **Session Owner Selection** is set to **First Packet**). □ FW1 uses the configured session setup load-sharing option to identify the session setup firewall. In this example, FW2 is configured to perform session setup. □ FW1 uses the HA3 link to send the first packet to FW2. □ FW2 sets up the session and returns the packet to FW1 for Layer 7 processing, if any. □ FW1 then forwards the packet out the egress interface to the destination. **Source:** *PAN-OS Administrator's Guide, Pg. 222*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 Ingress Receive packet Packet Ingress process Extract L2/L3/L4 information, Ingress interface/zone lookup, IP fragment reassembly if applicable Discard packet Y Ingress process error? N FW inspection applicable? Y IPSec/SSL-VPN tunnel packet? IPSec/SSL-VPN tunnel decryption N FW Session Setup/Slowpath FW Fastpath Firewall session lookup Session match found? Y Forwarding lookup Get egress interface/zone and VSYS from L3 route, L2 FDB lookup, etc L2-4 Firewall processing Discard packet if session not in active state, update session lifetime, do NAT if applicable NAT policy lookup Application Identification **Source:** https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081 **P.R. 3-1(g)**: If a party claiming patent infringement asserts that a claim element is a software limitation, the party need not comply with P.R. 3-1 for those claim elements until 30 days after source code for each Accused Instrumentality is produced by the opposing party. Accordingly, Implicit reserves the right to amend and/or supplement its identification and evidence with respect to this element.
1[E] determine a key value using information in the one or more packets;	The Accused System and Method determines a key value using information in a received packet. This key value is determined utilizing the App-ID inspection process, which interprets the different layers of a given message, and heuristic analyses. The identifiers of entities such as Sites, Applications, Flows, Classes, Rules, Policies, and other objects in the Accused System and Method are key values. Key values may be expressed as tuples or more complex data structures or collections of attributes.



App-ID Overview

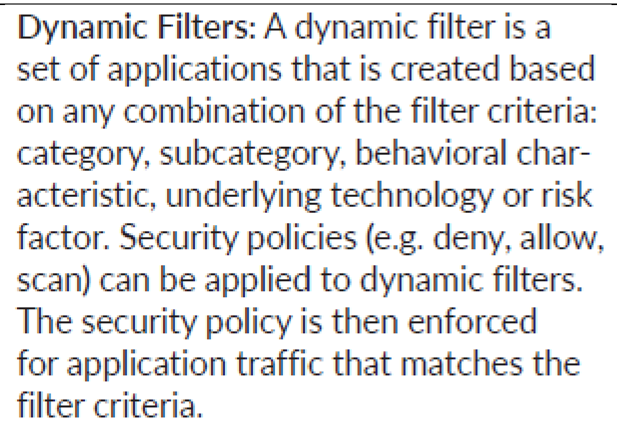
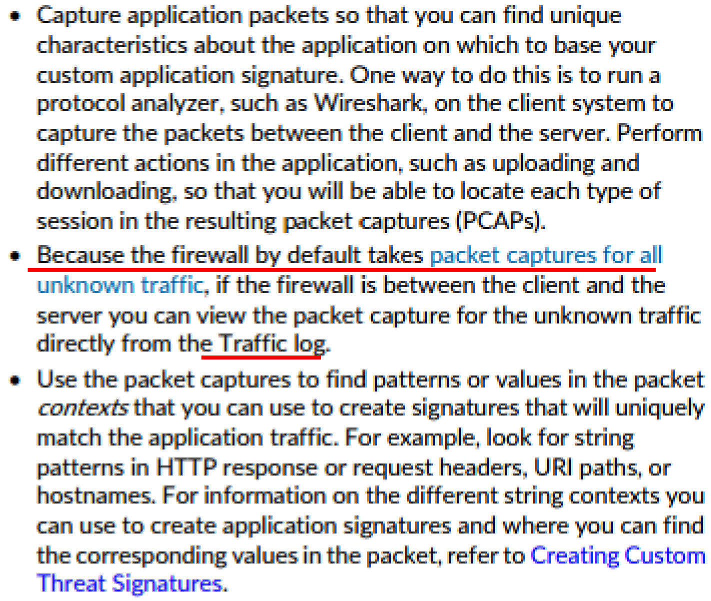
App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.

Here's how App-ID identifies applications traversing your network:

- Traffic is matched against policy to check whether it is allowed on the network.
- Signatures are then applied to allowed traffic to identify the application based on unique application properties and related transaction characteristics. The signature also determines if the application is being used on its default port or it is using a non-standard port. If the traffic is allowed by policy, the traffic is then scanned for threats and further analyzed for identifying the application more granularly.
- If App-ID determines that encryption (SSL or SSH) is in use, and a Decryption policy rule is in place, the session is decrypted and application signatures are applied again on the decrypted flow.
- Decoders for known protocols are then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (for example, Yahoo! Instant Messenger used across HTTP). Decoders validate that the traffic conforms to the protocol specification and provide support for NAT traversal and opening dynamic pinholes for applications such as SIP and FTP.
- For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics or behavioral analysis may be used to determine the identity of the application.

When the application is identified, the policy check determines how to treat the application, for example—block, or allow and scan for threats, inspect for unauthorized file transfer and data patterns, or shape using QoS.

Source: *PAN-OS Administrator's Guide, Pg. 474,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 Dynamic Filters: A dynamic filter is a set of applications that is created based on any combination of the filter criteria: category, subcategory, behavioral characteristic, underlying technology or risk factor. Security policies (e.g. deny, allow, scan) can be applied to dynamic filters. The security policy is then enforced for application traffic that matches the filter criteria. *App-ID Tech Brief*, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/app-id-tech-brief  • Capture application packets so that you can find unique characteristics about the application on which to base your custom application signature. One way to do this is to run a protocol analyzer, such as Wireshark, on the client system to capture the packets between the client and the server. Perform different actions in the application, such as uploading and downloading, so that you will be able to locate each type of session in the resulting packet captures (PCAPs). • Because the firewall by default takes packet captures for all unknown traffic, if the firewall is between the client and the server you can view the packet capture for the unknown traffic directly from the Traffic log. • Use the packet captures to find patterns or values in the packet *contexts* that you can use to create signatures that will uniquely match the application traffic. For example, look for string patterns in HTTP response or request headers, URI paths, or hostnames. For information on the different string contexts you can use to create application signatures and where you can find the corresponding values in the packet, refer to Creating Custom Threat Signatures. **Source:** *PAN-OS Administrator's Guide, Pg. 485*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

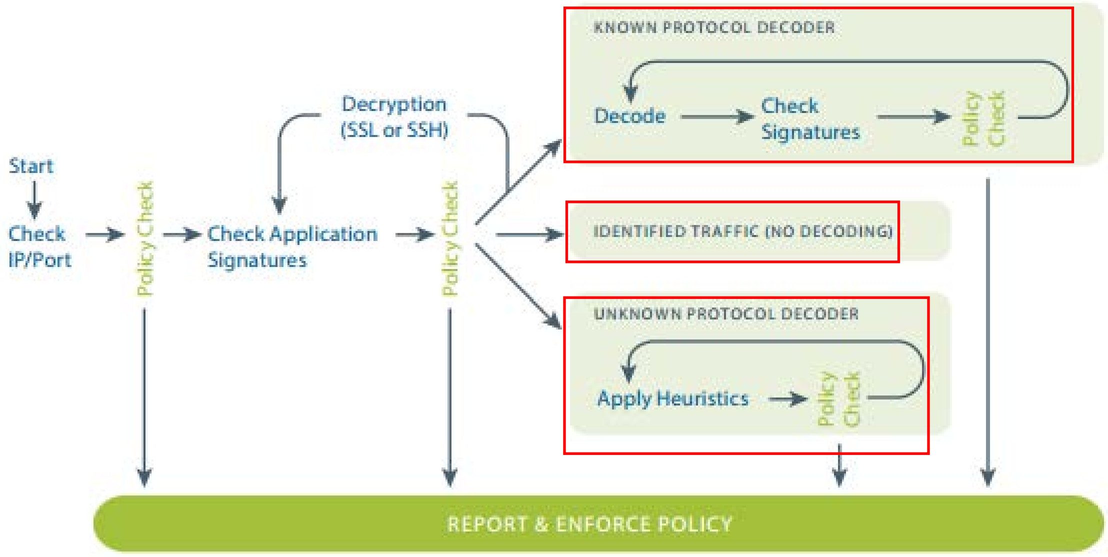
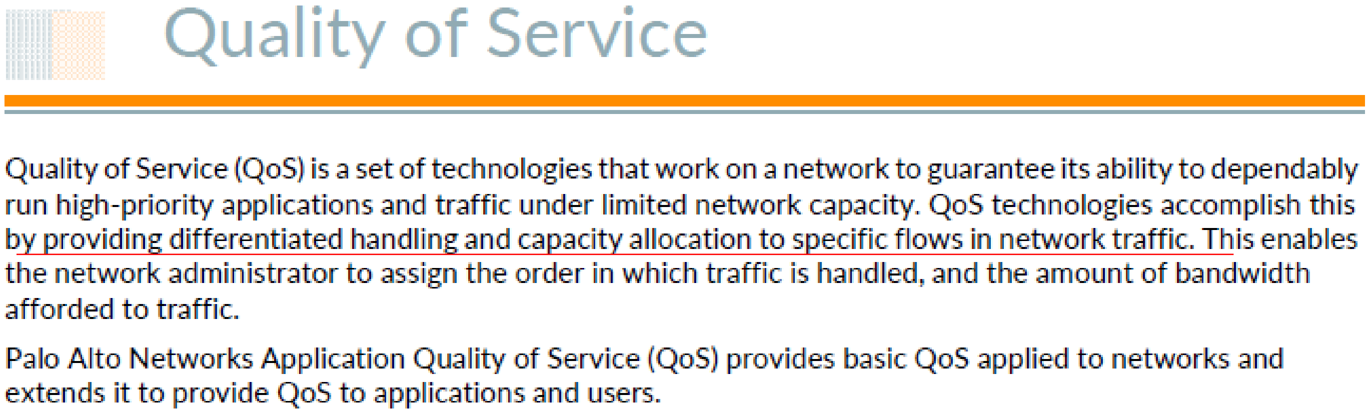


Figure 1: How App-ID classifies traffic.

App-ID Tech Brief, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/app-id-tech-brief



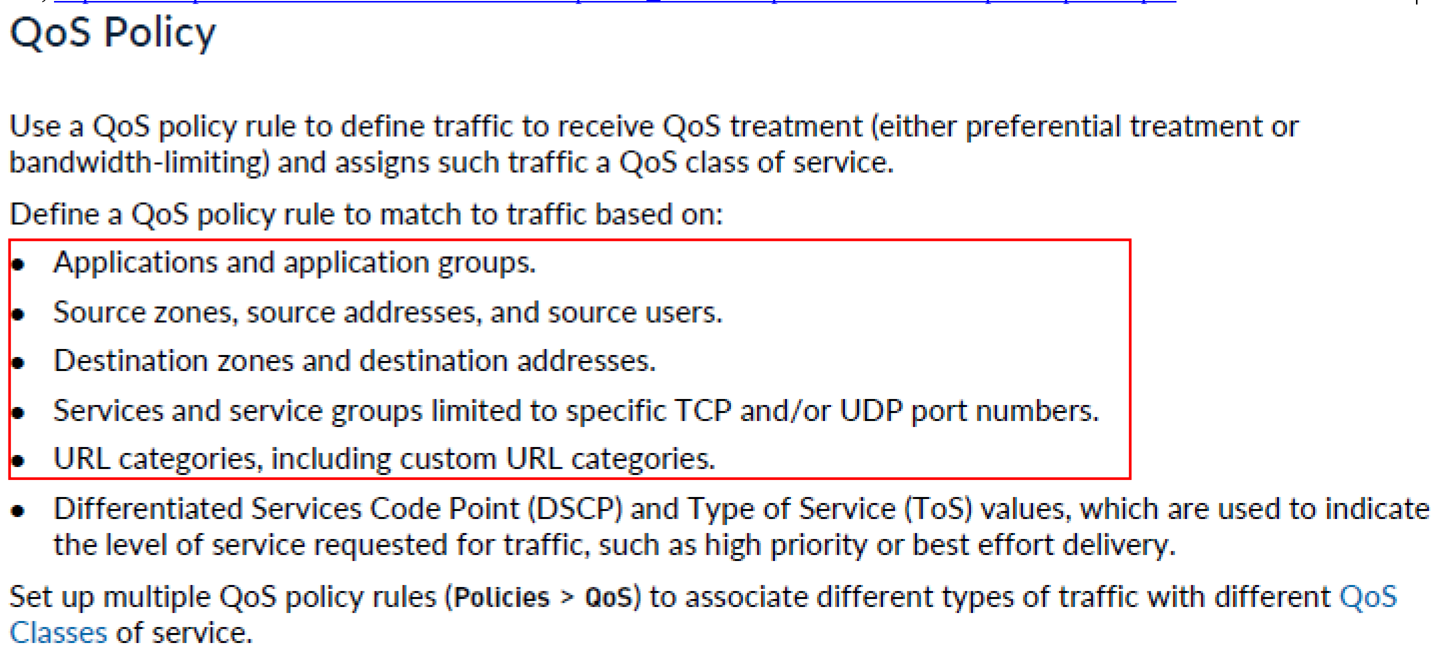
Quality of Service

Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which traffic is handled, and the amount of bandwidth afforded to traffic.

Palo Alto Networks Application Quality of Service (QoS) provides basic QoS applied to networks and extends it to provide QoS to applications and users.

Source: *PAN-OS Administrator's Guide, Pg.*

647, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf



QoS Policy

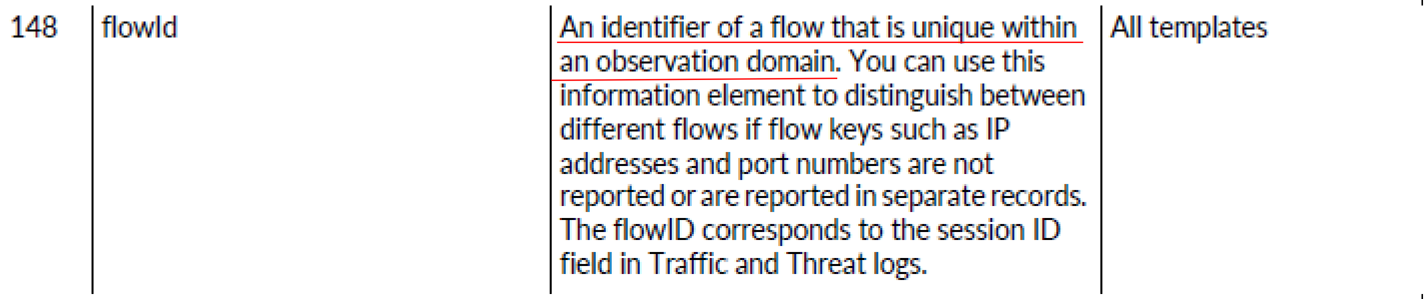
Use a QoS policy rule to define traffic to receive QoS treatment (either preferential treatment or bandwidth-limiting) and assigns such traffic a QoS class of service.

Define a QoS policy rule to match to traffic based on:

- Applications and application groups.
- Source zones, source addresses, and source users.
- Destination zones and destination addresses.
- Services and service groups limited to specific TCP and/or UDP port numbers.
- URL categories, including custom URL categories.
- Differentiated Services Code Point (DSCP) and Type of Service (ToS) values, which are used to indicate the level of service requested for traffic, such as high priority or best effort delivery.

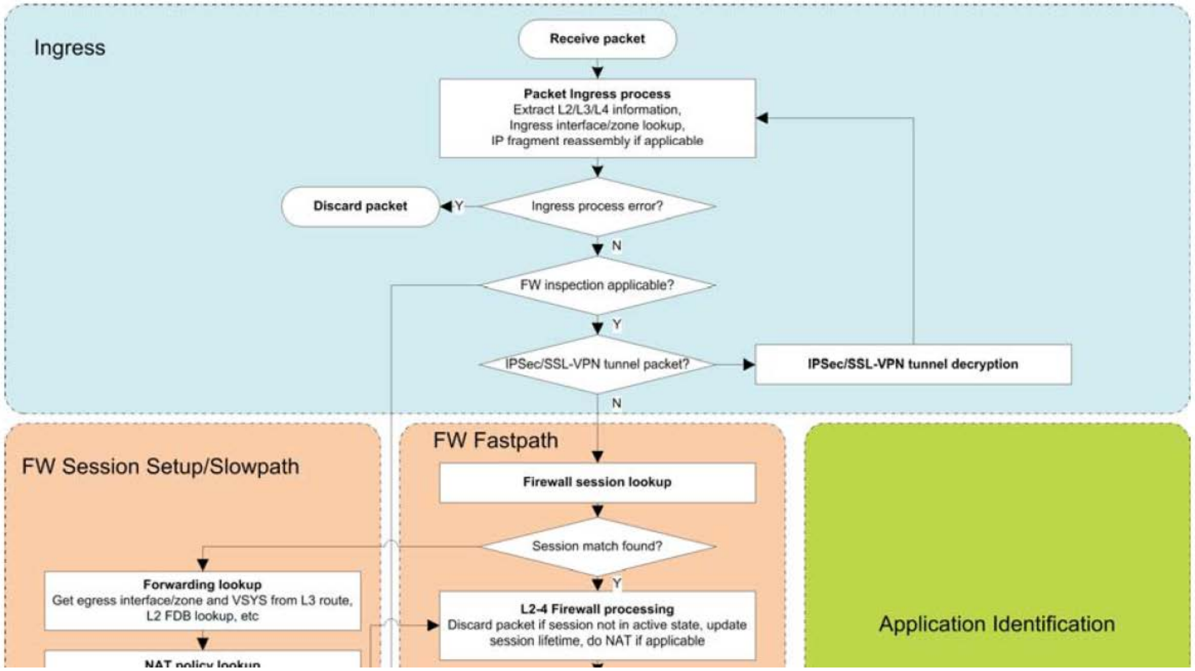
Set up multiple QoS policy rules (**Policies > QoS**) to associate different types of traffic with different QoS Classes of service.

Source: *PAN-OS Administrator's Guide, Pg. 650,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

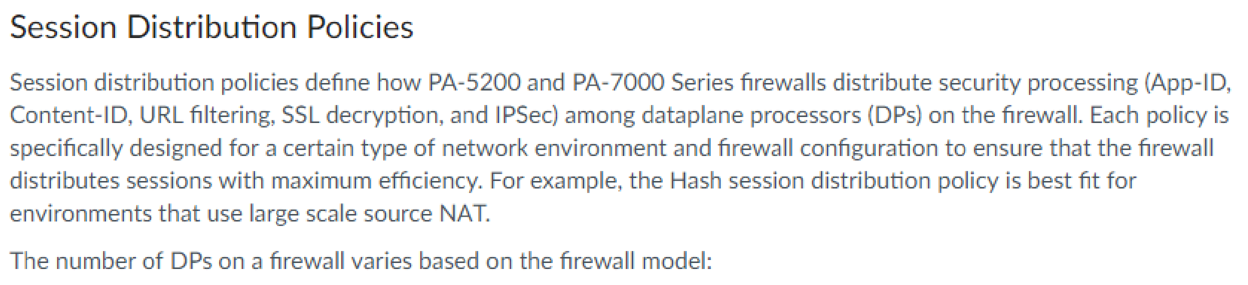


148	flowId	An identifier of a flow that is unique within an observation domain. You can use this information element to distinguish between different flows if flow keys such as IP addresses and port numbers are not reported or are reported in separate records. The flowID corresponds to the session ID field in Traffic and Threat logs.	All templates

Source: *PAN-OS Administrator's Guide, Pg. 400,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf


Ingress
Receive packet
Packet Ingress process
Extract L2/L3/L4 information,
Ingress interface/zone lookup,
IP fragment reassembly if applicable
Discard packet
Y
Ingress process error?
N
FW inspection applicable?
Y
IPSec/SSL-VPN tunnel packet?
IPSec/SSL-VPN tunnel decryption
N
FW Session Setup/Slowpath
FW Fastpath
Firewall session lookup
Session match found?
Y
Forwarding lookup
Get egress interface/zone and VSYS from L3 route,
L2 FDB lookup, etc
L2-4 Firewall processing
Discard packet if session not in active state, update session lifetime, do NAT if applicable
NAT policy lookup
Application Identification

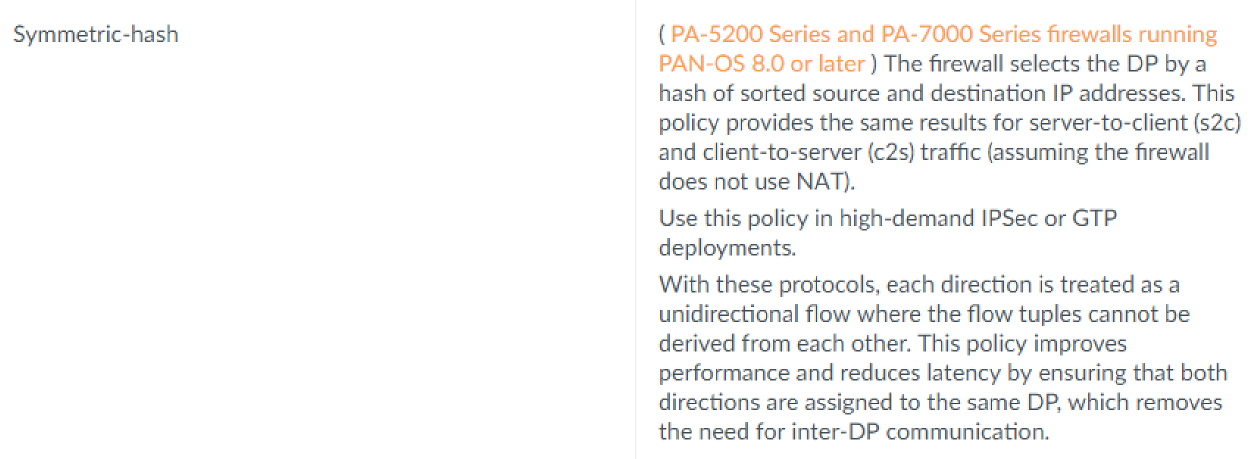
Source: https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

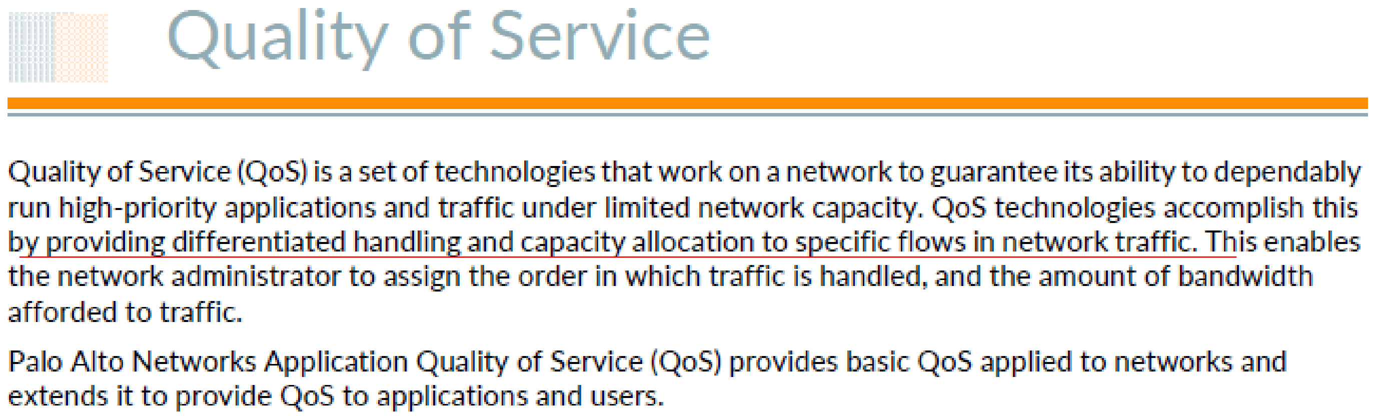


Session Distribution Policies

Session distribution policies define how PA-5200 and PA-7000 Series firewalls distribute security processing (App-ID, Content-ID, URL filtering, SSL decryption, and IPSec) among dataplane processors (DPs) on the firewall. Each policy is specifically designed for a certain type of network environment and firewall configuration to ensure that the firewall distributes sessions with maximum efficiency. For example, the Hash session distribution policy is best fit for environments that use large scale source NAT.

The number of DPs on a firewall varies based on the firewall model:

	 Symmetric-hash (PA-5200 Series and PA-7000 Series firewalls running PAN-OS 8.0 or later) The firewall selects the DP by a hash of sorted source and destination IP addresses. This policy provides the same results for server-to-client (s2c) and client-to-server (c2s) traffic (assuming the firewall does not use NAT). Use this policy in high-demand IPSec or GTP deployments. With these protocols, each direction is treated as a unidirectional flow where the flow tuples cannot be derived from each other. This policy improves performance and reduces latency by ensuring that both directions are assigned to the same DP, which removes the need for inter-DP communication. **Source:** https://www.paloaltonetworks.com/documentation/80/pan-os/pan-os/networking/session-distribution-policies **P.R. 3-1(g)**: If a party claiming patent infringement asserts that a claim element is a software limitation, the party need not comply with P.R. 3-1 for those claim elements until 30 days after source code for each Accused Instrumentality is produced by the opposing party. Accordingly, Implicit reserves the right to amend and/or supplement its identification and evidence with respect to this element.
1[F] identify, using the key value, a sequence of two or more routines, wherein the sequence includes a routine that is used to execute a Transmission Control Protocol (TCP) to process packets having a TCP format;	The Accused System and Method identifies a sequence of routines by using the key value previously determined. The sequence of routines includes a routine that is executable to perform a Transmission Control Protocol (TCP) routine to convert at least one of the packets of the message into a different format.

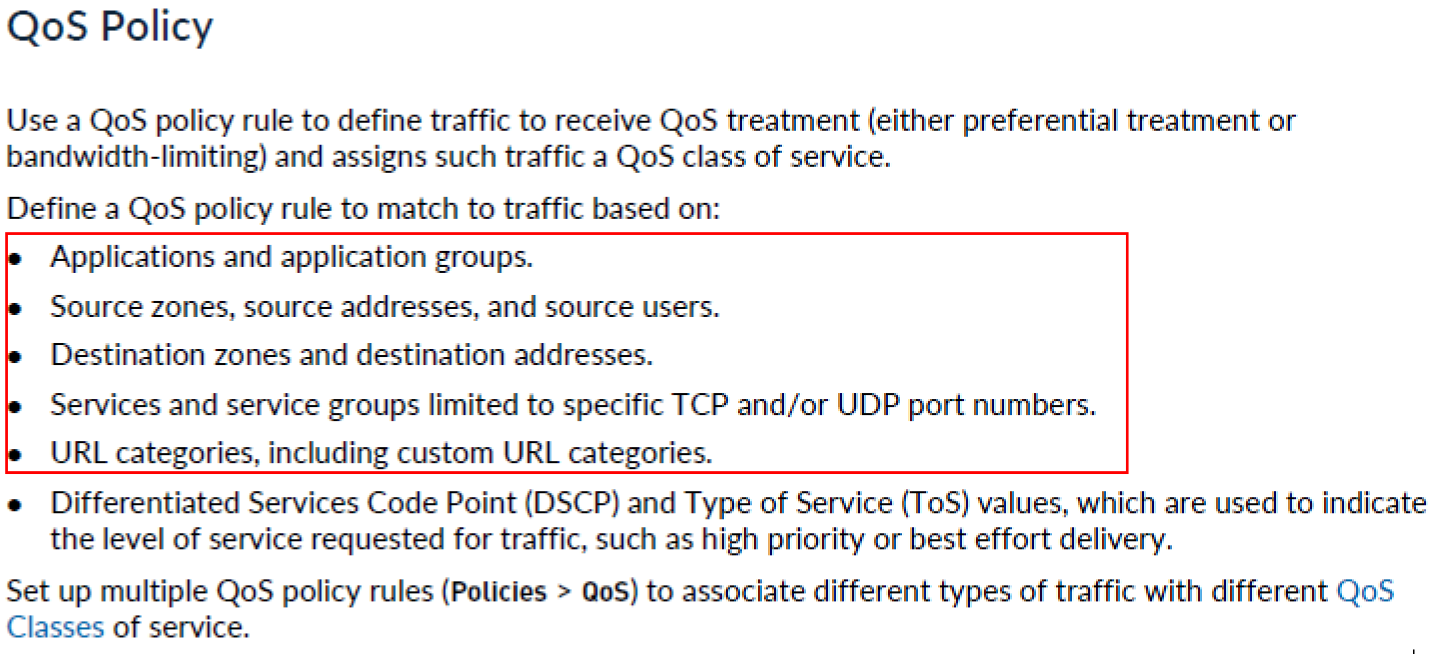


Quality of Service

Quality of Service (QoS) is a set of technologies that work on a network to guarantee its ability to dependably run high-priority applications and traffic under limited network capacity. QoS technologies accomplish this by providing differentiated handling and capacity allocation to specific flows in network traffic. This enables the network administrator to assign the order in which traffic is handled, and the amount of bandwidth afforded to traffic.

Palo Alto Networks Application Quality of Service (QoS) provides basic QoS applied to networks and extends it to provide QoS to applications and users.

Source: *PAN-OS Administrator's Guide, Pg. 647*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf



QoS Policy

Use a QoS policy rule to define traffic to receive QoS treatment (either preferential treatment or bandwidth-limiting) and assigns such traffic a QoS class of service.

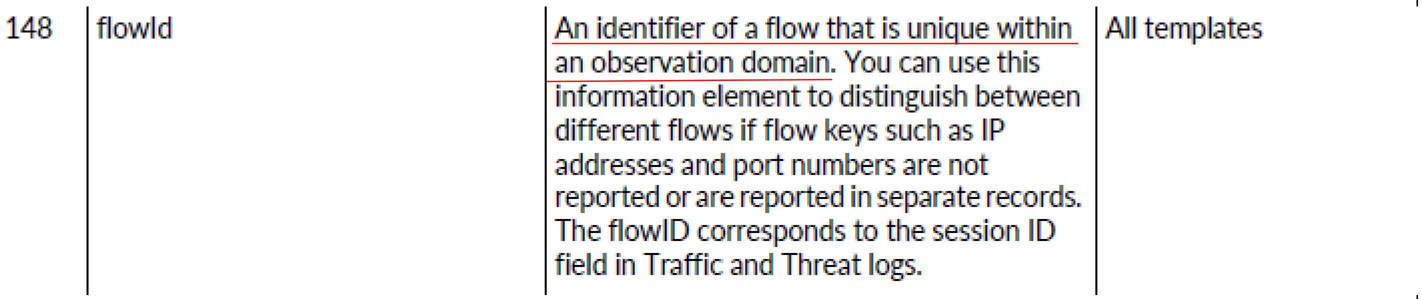
Define a QoS policy rule to match to traffic based on:

- Applications and application groups.
- Source zones, source addresses, and source users.
- Destination zones and destination addresses.
- Services and service groups limited to specific TCP and/or UDP port numbers.
- URL categories, including custom URL categories.
- Differentiated Services Code Point (DSCP) and Type of Service (ToS) values, which are used to indicate the level of service requested for traffic, such as high priority or best effort delivery.

Set up multiple QoS policy rules (**Policies > QoS**) to associate different types of traffic with different QoS Classes of service.

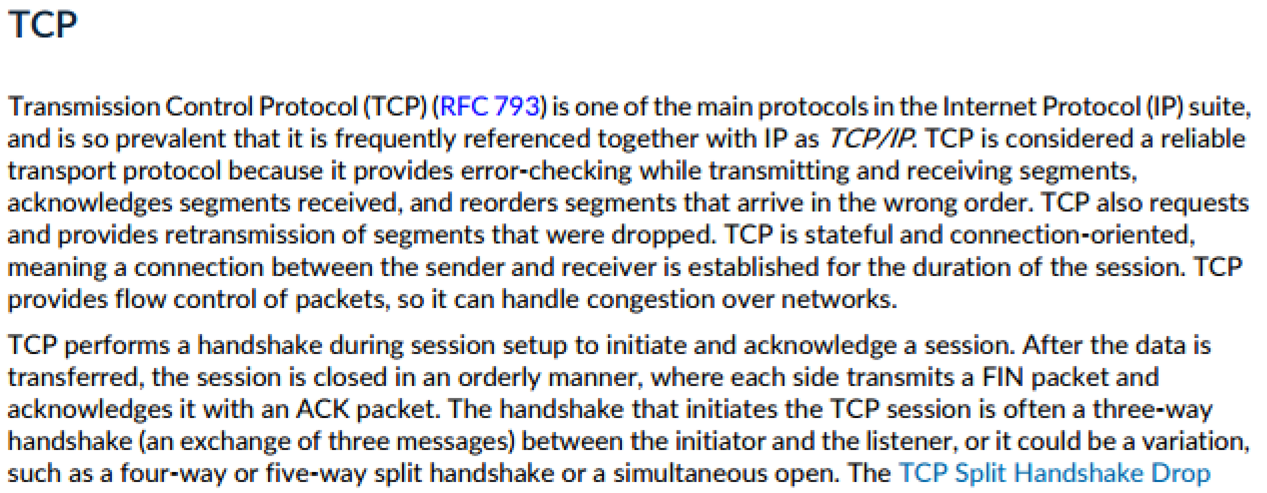
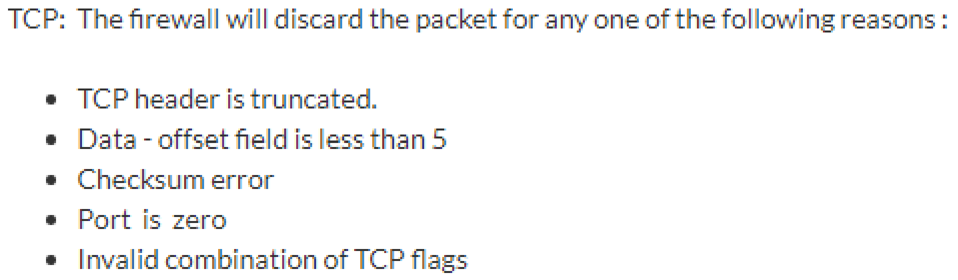
Source: *PAN-OS Administrator's Guide, Pg. 650*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

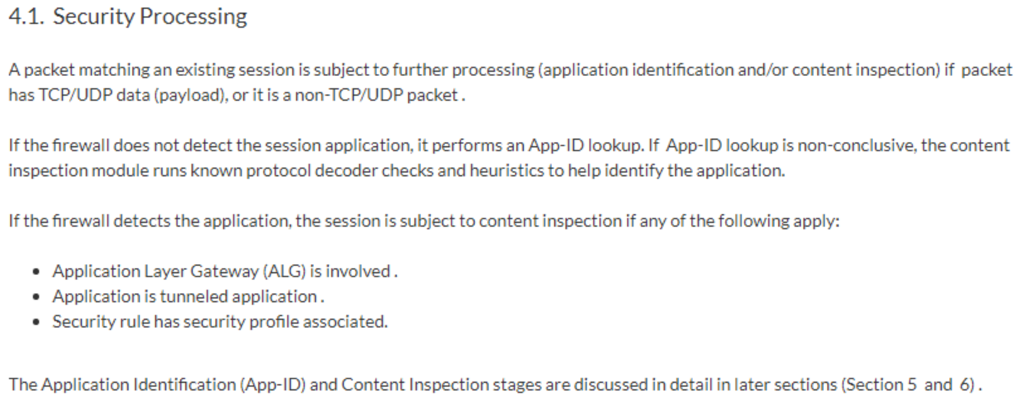
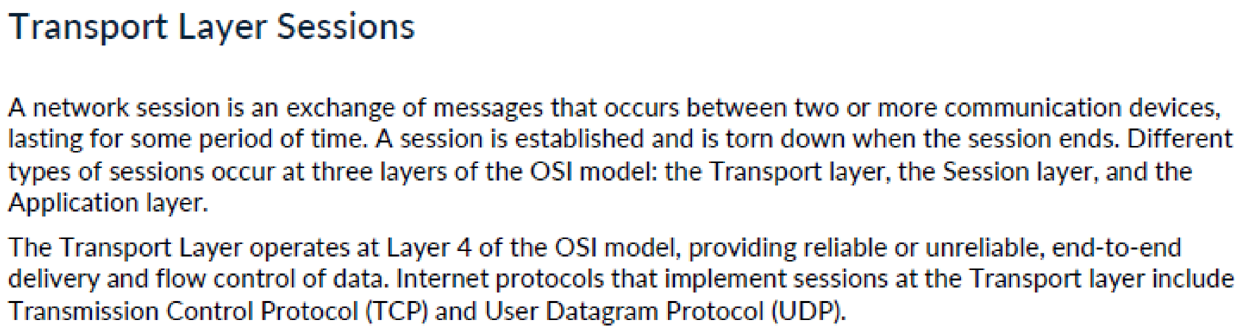
The definition of QoS and other rules and policies comprises a sequence of two or more routines for processing packets in a message, at least one of which requires converting data from TCP format to one or more intermediate formats for processing and/or analysis. QoS enforces, for example, complex routing priorities based on many parameters defined for an application or class. The identification of traffic as belonging to an application or other QoS policy addressable unit and the enforcement of QoS policies requires the execution of many routines to classify and route traffic. These may be stored as pure data structures (in code or a data store), as in a rules engine implementation or equivalent or as is typical in systems built using functional programming languages, or they may be stored as parametrized routines in which the execution of the same code with different inputs yields different results.

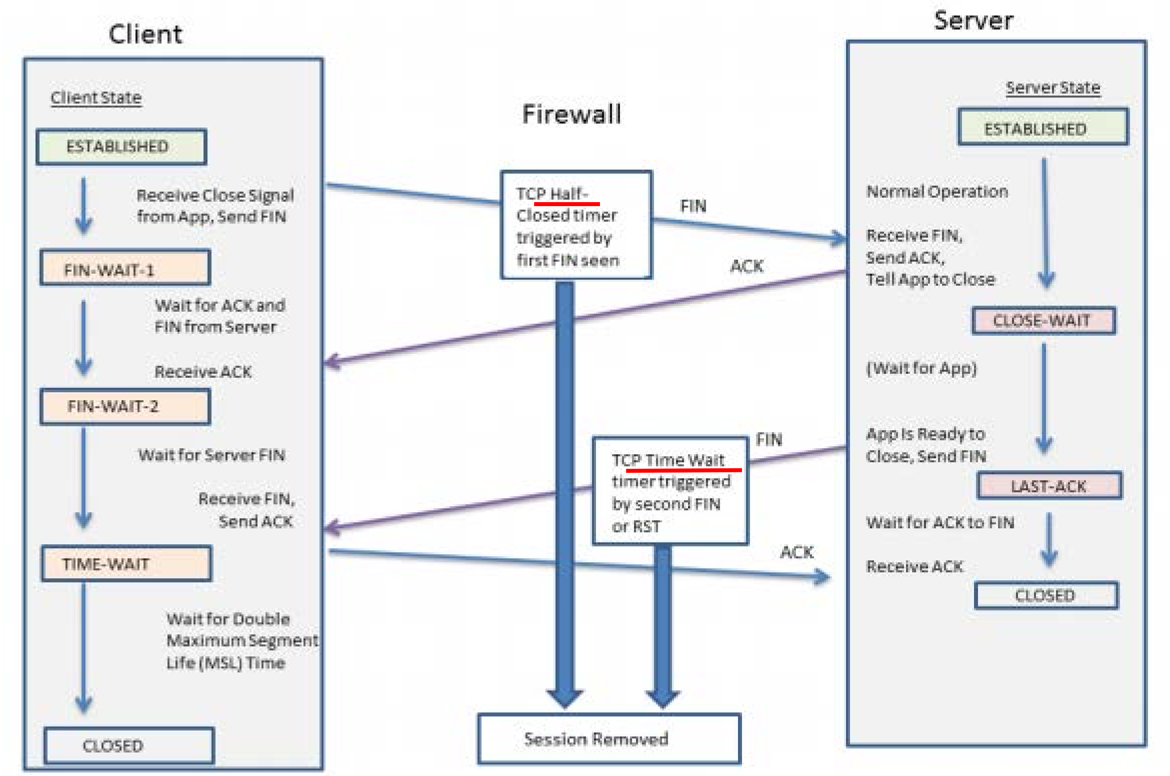


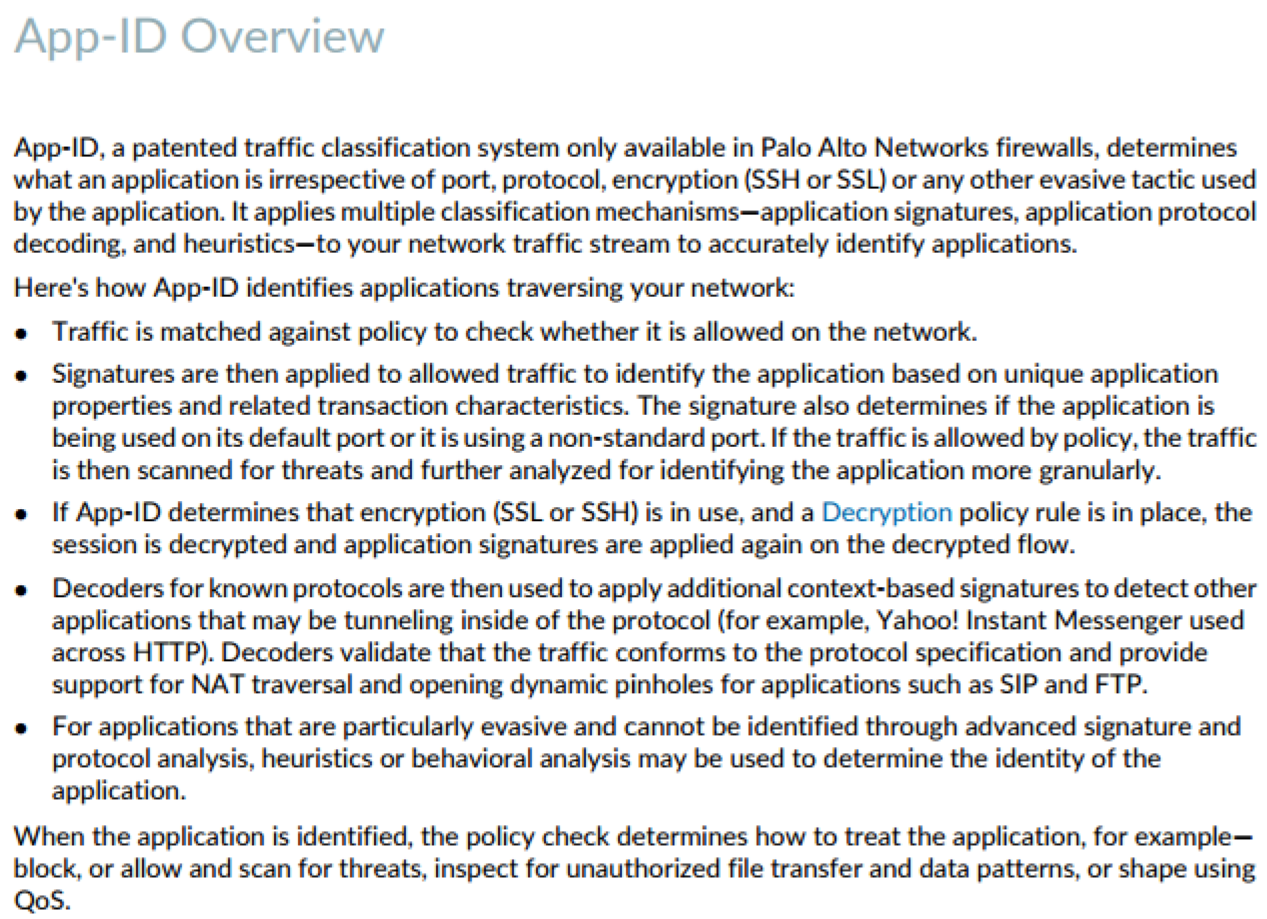
148	flowId	An identifier of a flow that is unique within an observation domain. You can use this information element to distinguish between different flows if flow keys such as IP addresses and port numbers are not reported or are reported in separate records. The flowID corresponds to the session ID field in Traffic and Threat logs.	All templates

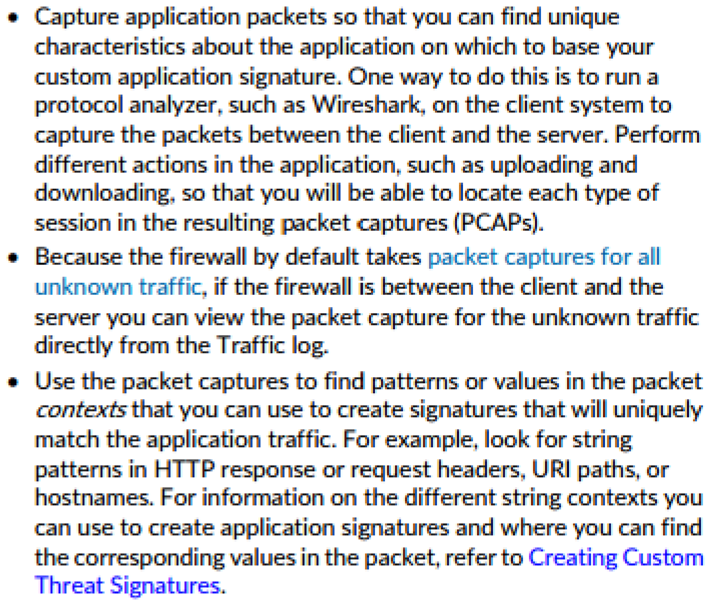
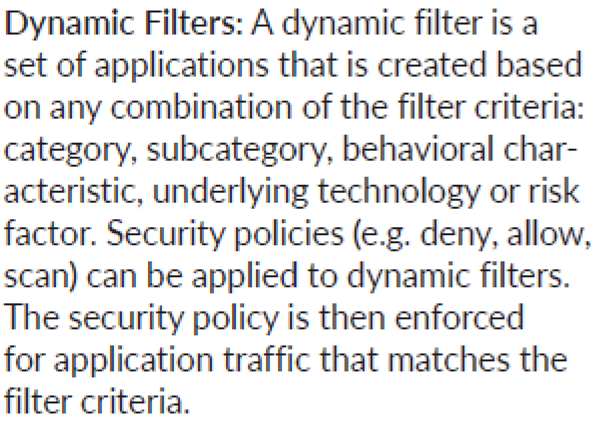
Source: *PAN-OS Administrator's Guide, Pg. 400,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

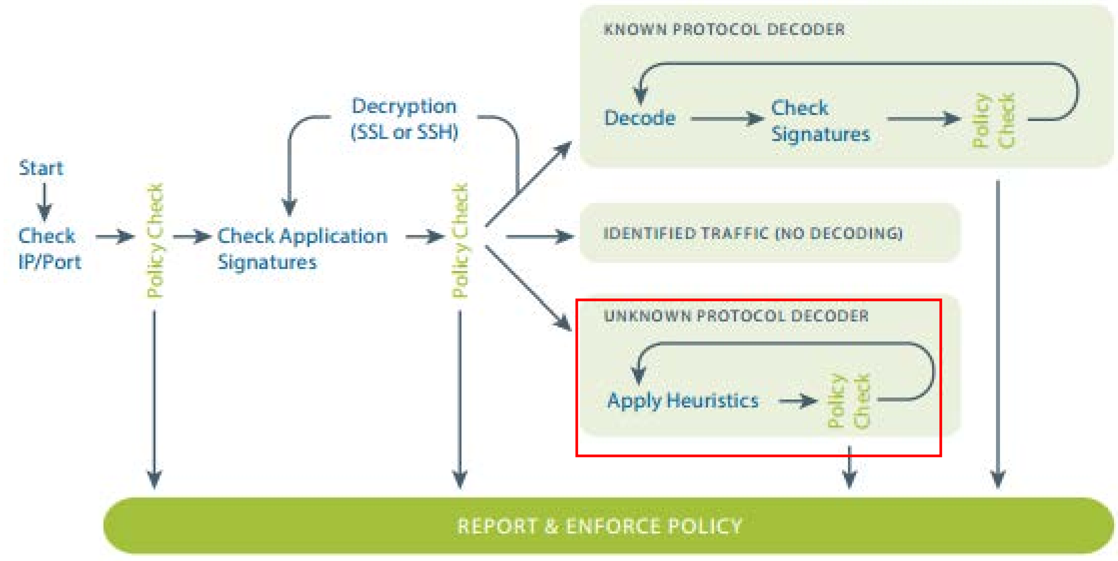
	 **TCP** Transmission Control Protocol (TCP) (RFC 793) is one of the main protocols in the Internet Protocol (IP) suite, and is so prevalent that it is frequently referenced together with IP as *TCP/IP*. TCP is considered a reliable transport protocol because it provides error-checking while transmitting and receiving segments, acknowledges segments received, and reorders segments that arrive in the wrong order. TCP also requests and provides retransmission of segments that were dropped. TCP is stateful and connection-oriented, meaning a connection between the sender and receiver is established for the duration of the session. TCP provides flow control of packets, so it can handle congestion over networks. TCP performs a handshake during session setup to initiate and acknowledge a session. After the data is transferred, the session is closed in an orderly manner, where each side transmits a FIN packet and acknowledges it with an ACK packet. The handshake that initiates the TCP session is often a three-way handshake (an exchange of three messages) between the initiator and the listener, or it could be a variation, such as a four-way or five-way split handshake or a simultaneous open. The TCP Split Handshake Drop **Source:** *PAN-OS Administrator's Guide, Pg. 914*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf  TCP: The firewall will discard the packet for any one of the following reasons : • TCP header is truncated. • Data - offset field is less than 5 • Checksum error • Port is zero • Invalid combination of TCP flags **Source:** https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

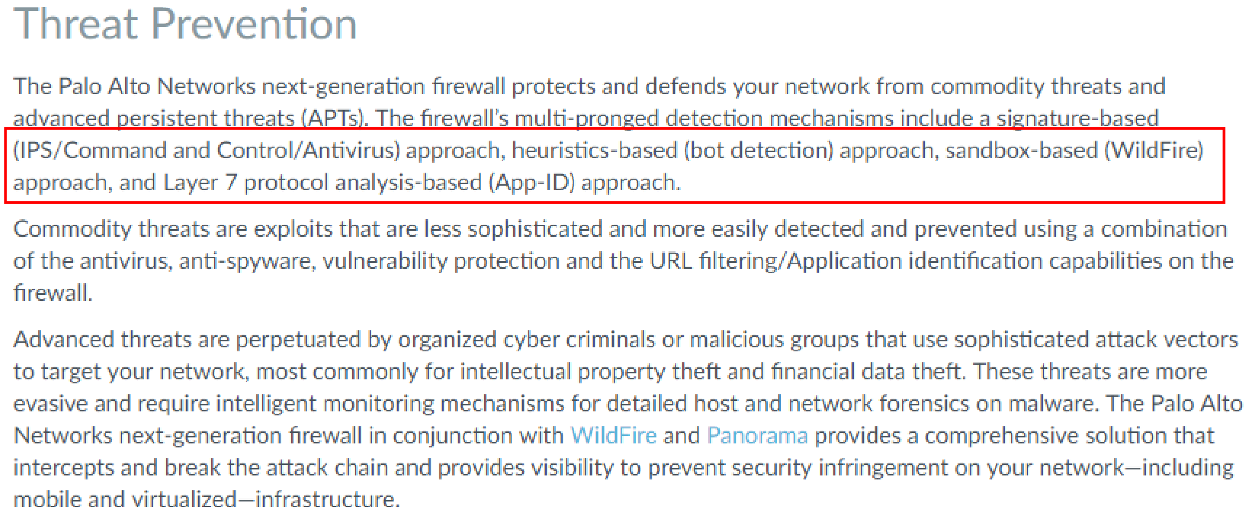
	 4.1. Security Processing A packet matching an existing session is subject to further processing (application identification and/or content inspection) if packet has TCP/UDP data (payload), or it is a non-TCP/UDP packet . If the firewall does not detect the session application, it performs an App-ID lookup. If App-ID lookup is non-conclusive, the content inspection module runs known protocol decoder checks and heuristics to help identify the application. If the firewall detects the application, the session is subject to content inspection if any of the following apply: • Application Layer Gateway (ALG) is involved . • Application is tunneled application . • Security rule has security profile associated. The Application Identification (App-ID) and Content Inspection stages are discussed in detail in later sections (Section 5 and 6) . **Source:** https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081  Transport Layer Sessions A network session is an exchange of messages that occurs between two or more communication devices, lasting for some period of time. A session is established and is torn down when the session ends. Different types of sessions occur at three layers of the OSI model: the Transport layer, the Session layer, and the Application layer. The Transport Layer operates at Layer 4 of the OSI model, providing reliable or unreliable, end-to-end delivery and flow control of data. Internet protocols that implement sessions at the Transport layer include Transmission Control Protocol (TCP) and User Datagram Protocol (UDP). **Source:** *PAN-OS Administrator’s Guide, Pg. 914*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

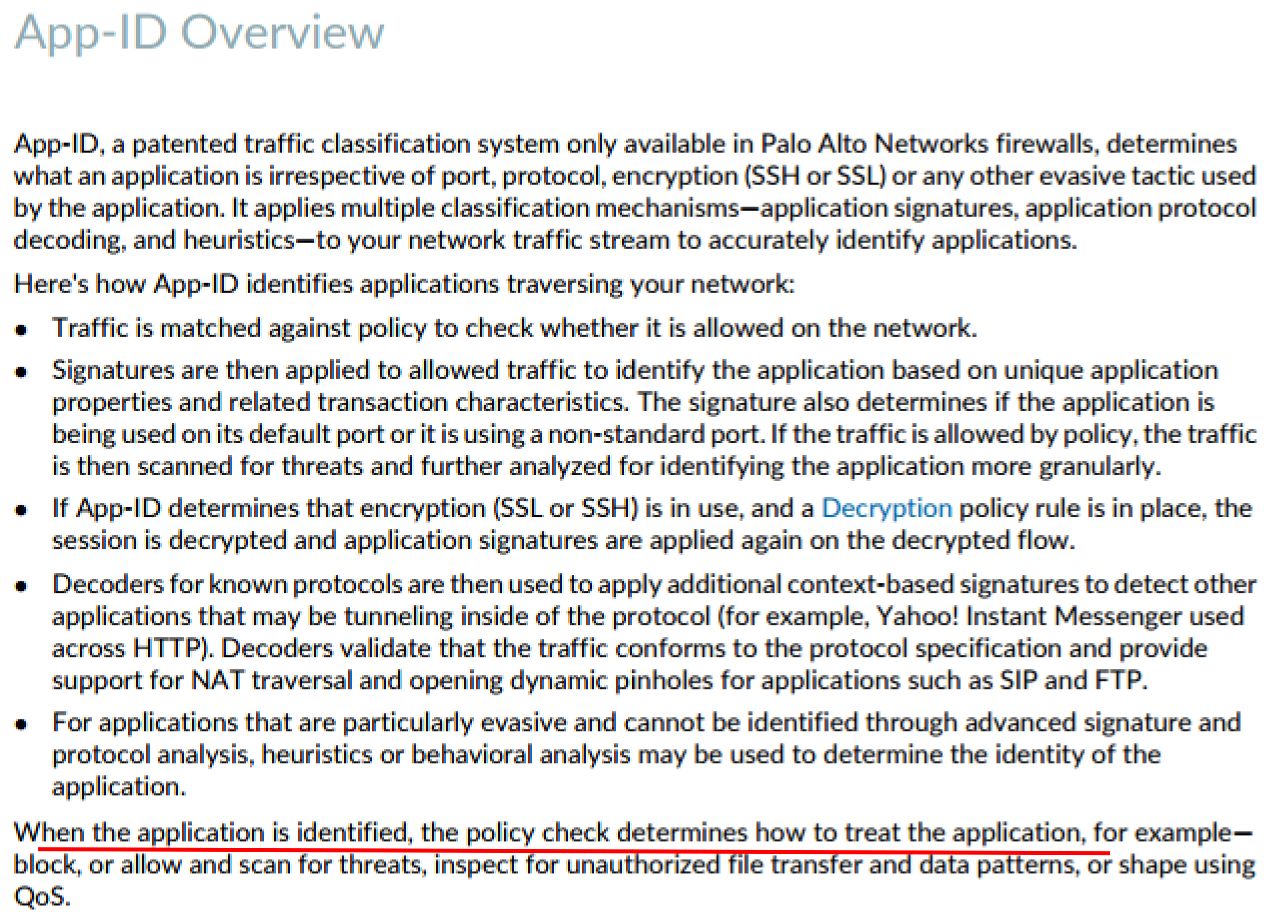
	 Client Client State ESTABLISHED Receive Close Signal from App, Send FIN FIN-WAIT-1 Wait for ACK and FIN from Server Receive ACK FIN-WAIT-2 Wait for Server FIN Receive FIN, Send ACK TIME-WAIT Wait for Double Maximum Segment Life (MSL) Time CLOSED Firewall TCP Half-Closed timer triggered by first FIN seen FIN ACK TCP Time Wait timer triggered by second FIN or RST FIN ACK Session Removed Server Server State ESTABLISHED Normal Operation Receive FIN, Send ACK, Tell App to Close CLOSE-WAIT (Wait for App) App Is Ready to Close, Send FIN LAST-ACK Wait for ACK to FIN Receive ACK CLOSED **Source:** *PAN-OS Administrator's Guide, Pg. 916,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf **P.R. 3-1(g)**: If a party claiming patent infringement asserts that a claim element is a software limitation, the party need not comply with P.R. 3-1 for those claim elements until 30 days after source code for each Accused Instrumentality is produced by the opposing party. Accordingly, Implicit reserves the right to amend and/or supplement its identification and evidence with respect to this element.
1[G] create a path that includes one or more data structures that indicate the identified sequence of two or	The Accused System and Method includes instructions to create a path that includes one or more data structures that indicate a sequence of routines. The created path is message-specific, thus state information is stored in the path. This may take one or several of many forms, such as progress records, log entries, transient or stateful code

more routines, wherein the path is usable to store state information associated with the message; and	attributes, database entries, or other data indicating processing progress or results for a message.  App-ID Overview App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications. Here's how App-ID identifies applications traversing your network: • Traffic is matched against policy to check whether it is allowed on the network. • Signatures are then applied to allowed traffic to identify the application based on unique application properties and related transaction characteristics. The signature also determines if the application is being used on its default port or it is using a non-standard port. If the traffic is allowed by policy, the traffic is then scanned for threats and further analyzed for identifying the application more granularly. • If App-ID determines that encryption (SSL or SSH) is in use, and a Decryption policy rule is in place, the session is decrypted and application signatures are applied again on the decrypted flow. • Decoders for known protocols are then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (for example, Yahoo! Instant Messenger used across HTTP). Decoders validate that the traffic conforms to the protocol specification and provide support for NAT traversal and opening dynamic pinholes for applications such as SIP and FTP. • For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics or behavioral analysis may be used to determine the identity of the application. When the application is identified, the policy check determines how to treat the application, for example—block, or allow and scan for threats, inspect for unauthorized file transfer and data patterns, or shape using QoS. **Source:** *PAN-OS Administrator's Guide, Pg. 474*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 • Capture application packets so that you can find unique characteristics about the application on which to base your custom application signature. One way to do this is to run a protocol analyzer, such as Wireshark, on the client system to capture the packets between the client and the server. Perform different actions in the application, such as uploading and downloading, so that you will be able to locate each type of session in the resulting packet captures (PCAPs). • Because the firewall by default takes packet captures for all unknown traffic, if the firewall is between the client and the server you can view the packet capture for the unknown traffic directly from the Traffic log. • Use the packet captures to find patterns or values in the packet *contexts* that you can use to create signatures that will uniquely match the application traffic. For example, look for string patterns in HTTP response or request headers, URI paths, or hostnames. For information on the different string contexts you can use to create application signatures and where you can find the corresponding values in the packet, refer to Creating Custom Threat Signatures. **Source:** *PAN-OS Administrator's Guide, Pg. 485*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf  Dynamic Filters: A dynamic filter is a set of applications that is created based on any combination of the filter criteria: category, subcategory, behavioral characteristic, underlying technology or risk factor. Security policies (e.g. deny, allow, scan) can be applied to dynamic filters. The security policy is then enforced for application traffic that matches the filter criteria. *App-ID Tech Brief*, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/app-id-tech-brief

	 Start Check IP/Port Policy Check Check Application Signatures Decryption (SSL or SSH) Policy Check KNOWN PROTOCOL DECODER Decode Check Signatures Policy Check IDENTIFIED TRAFFIC (NO DECODING) UNKNOWN PROTOCOL DECODER Apply Heuristics Policy Check REPORT & ENFORCE POLICY **Figure 1:** How App-ID classifies traffic. *App-ID Tech Brief*, https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/app-id-tech-brief

	 Threat Prevention The Palo Alto Networks next-generation firewall protects and defends your network from commodity threats and advanced persistent threats (APTs). The firewall's multi-pronged detection mechanisms include a signature-based (IPS/Command and Control/Antivirus) approach, heuristics-based (bot detection) approach, sandbox-based (WildFire) approach, and Layer 7 protocol analysis-based (App-ID) approach. Commodity threats are exploits that are less sophisticated and more easily detected and prevented using a combination of the antivirus, anti-spyware, vulnerability protection and the URL filtering/Application identification capabilities on the firewall. Advanced threats are perpetuated by organized cyber criminals or malicious groups that use sophisticated attack vectors to target your network, most commonly for intellectual property theft and financial data theft. These threats are more evasive and require intelligent monitoring mechanisms for detailed host and network forensics on malware. The Palo Alto Networks next-generation firewall in conjunction with WildFire and Panorama provides a comprehensive solution that intercepts and break the attack chain and provides visibility to prevent security infringement on your network—including mobile and virtualized—infrastructure. **Source:** https://www.paloaltonetworks.com/documentation/61/pan-os/pan-os/threat-prevention **P.R. 3-1(g)**: If a party claiming patent infringement asserts that a claim element is a software limitation, the party need not comply with P.R. 3-1 for those claim elements until 30 days after source code for each Accused Instrumentality is produced by the opposing party. Accordingly, Implicit reserves the right to amend and/or supplement its identification and evidence with respect to this element.
1[H] process subsequent packets in the message using the sequence of two or more routines indicated in the path.	The Accused System and Method processes subsequent packets in the message using the sequence of routines indicated in the path.



App-ID Overview

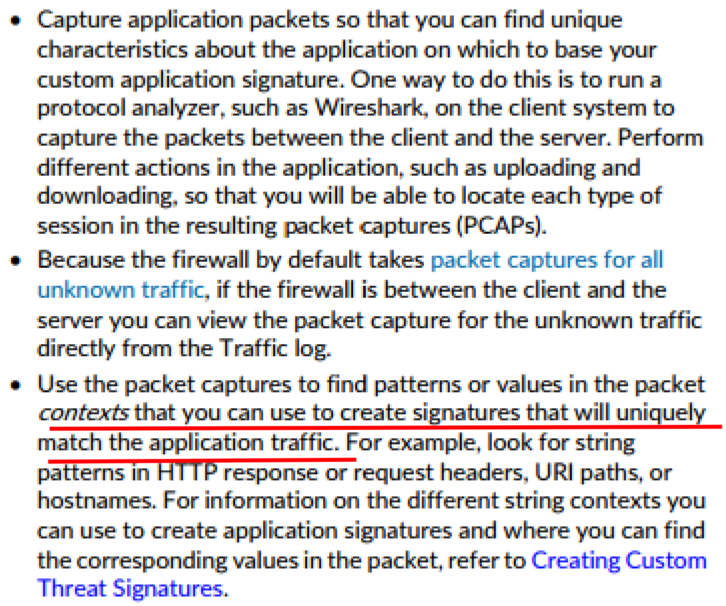
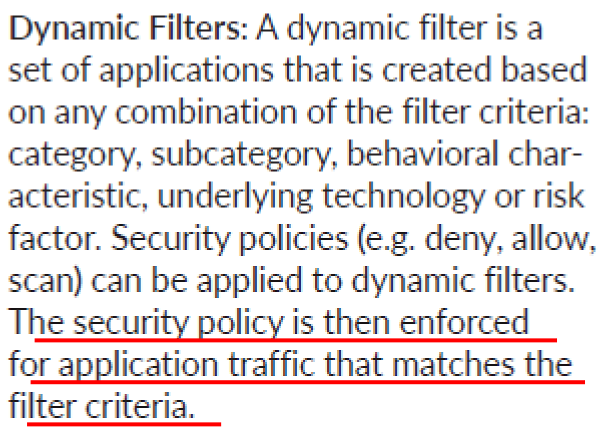
App-ID, a patented traffic classification system only available in Palo Alto Networks firewalls, determines what an application is irrespective of port, protocol, encryption (SSH or SSL) or any other evasive tactic used by the application. It applies multiple classification mechanisms—application signatures, application protocol decoding, and heuristics—to your network traffic stream to accurately identify applications.

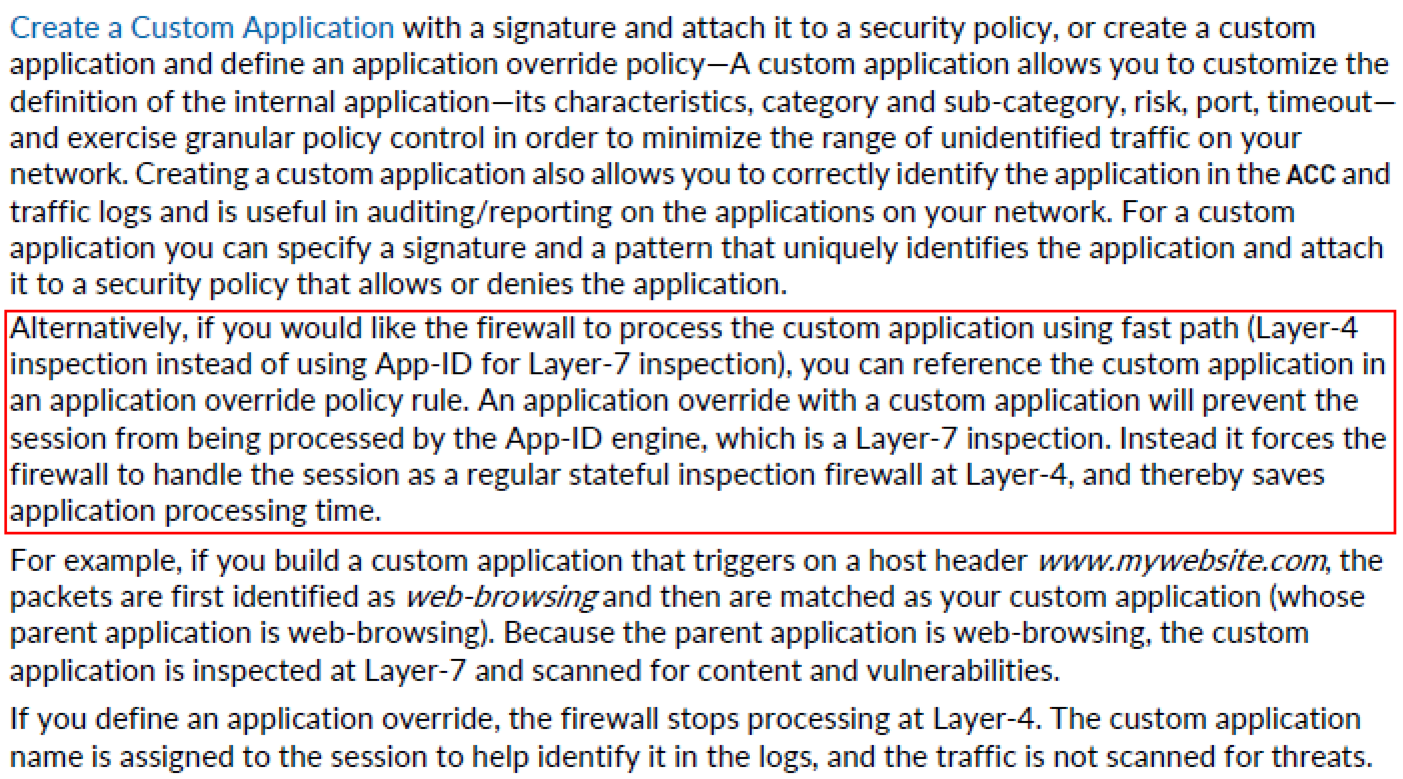
Here's how App-ID identifies applications traversing your network:

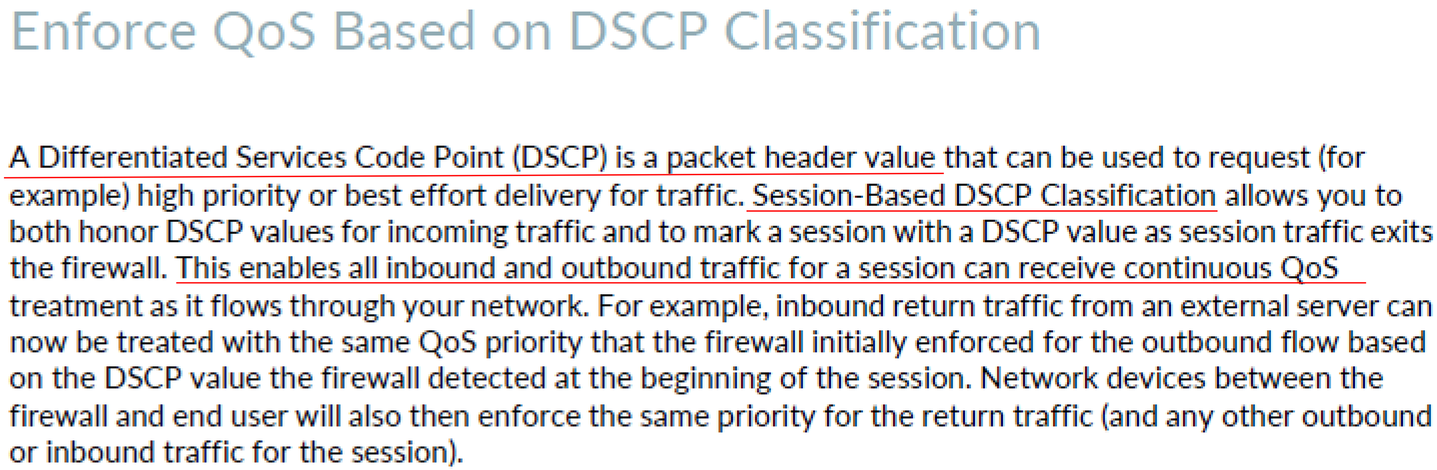
- Traffic is matched against policy to check whether it is allowed on the network.
- Signatures are then applied to allowed traffic to identify the application based on unique application properties and related transaction characteristics. The signature also determines if the application is being used on its default port or it is using a non-standard port. If the traffic is allowed by policy, the traffic is then scanned for threats and further analyzed for identifying the application more granularly.
- If App-ID determines that encryption (SSL or SSH) is in use, and a Decryption policy rule is in place, the session is decrypted and application signatures are applied again on the decrypted flow.
- Decoders for known protocols are then used to apply additional context-based signatures to detect other applications that may be tunneling inside of the protocol (for example, Yahoo! Instant Messenger used across HTTP). Decoders validate that the traffic conforms to the protocol specification and provide support for NAT traversal and opening dynamic pinholes for applications such as SIP and FTP.
- For applications that are particularly evasive and cannot be identified through advanced signature and protocol analysis, heuristics or behavioral analysis may be used to determine the identity of the application.

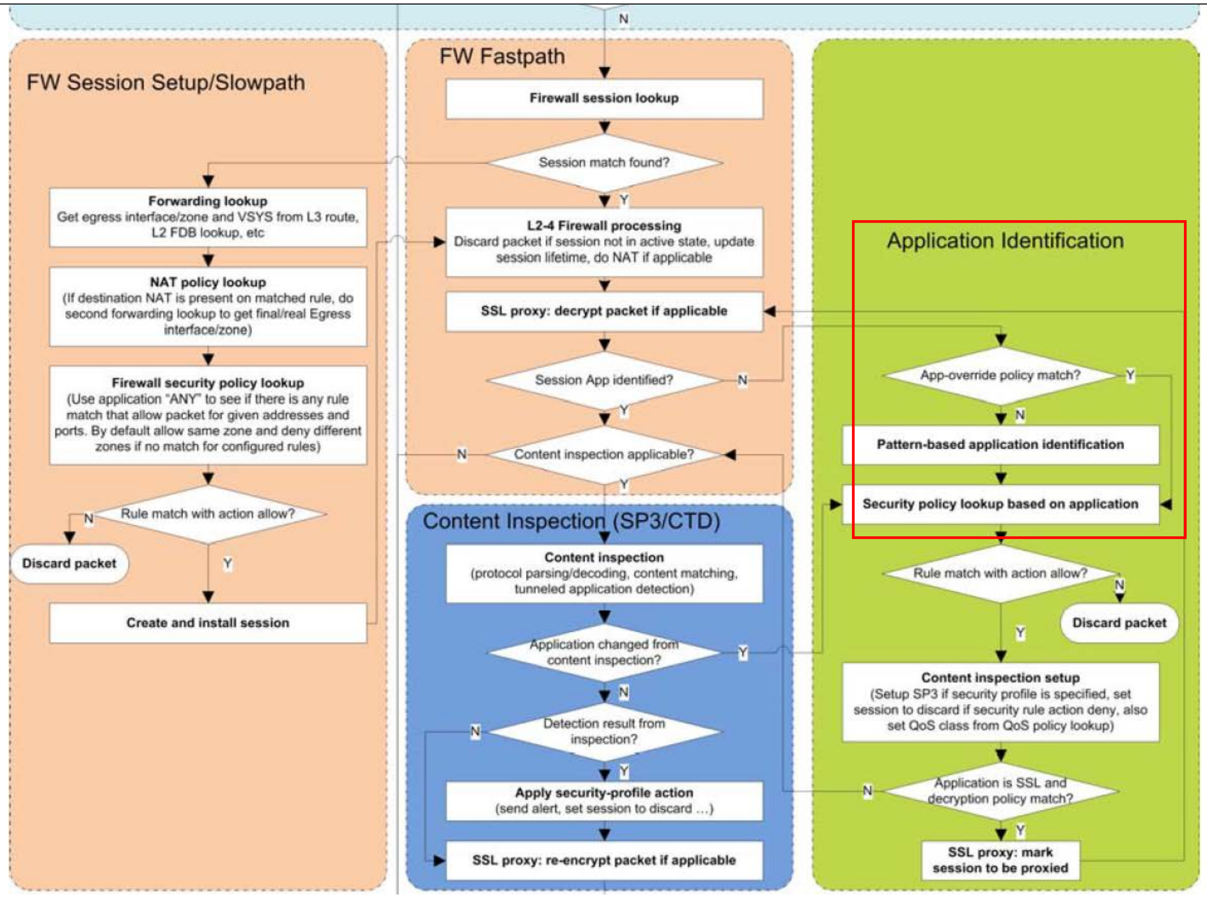
When the application is identified, the policy check determines how to treat the application, for example—block, or allow and scan for threats, inspect for unauthorized file transfer and data patterns, or shape using QoS.

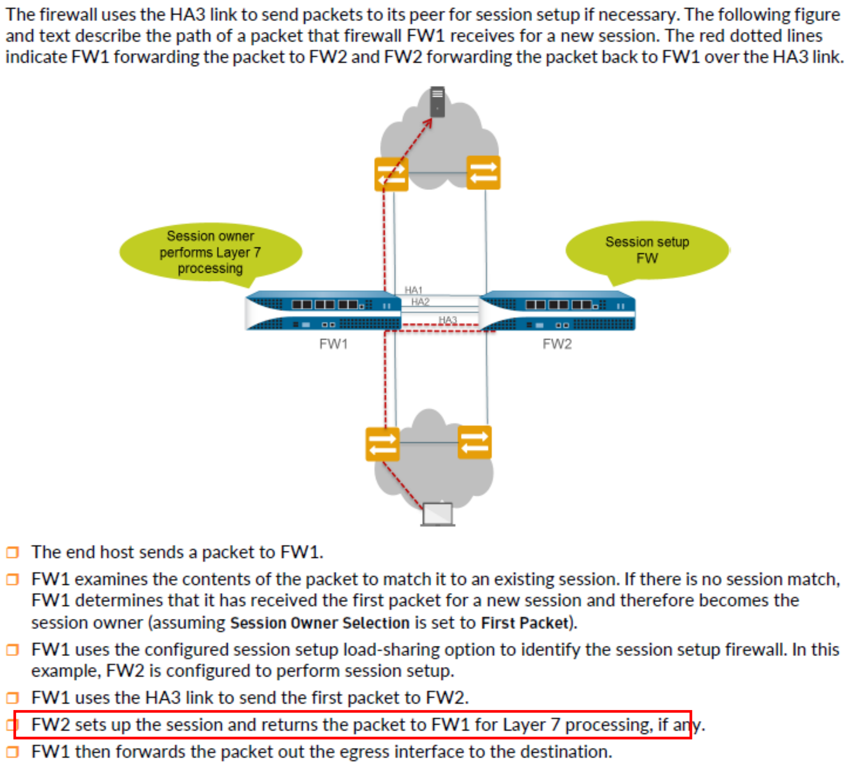
Source: *PAN-OS Administrator's Guide, Pg. 474,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

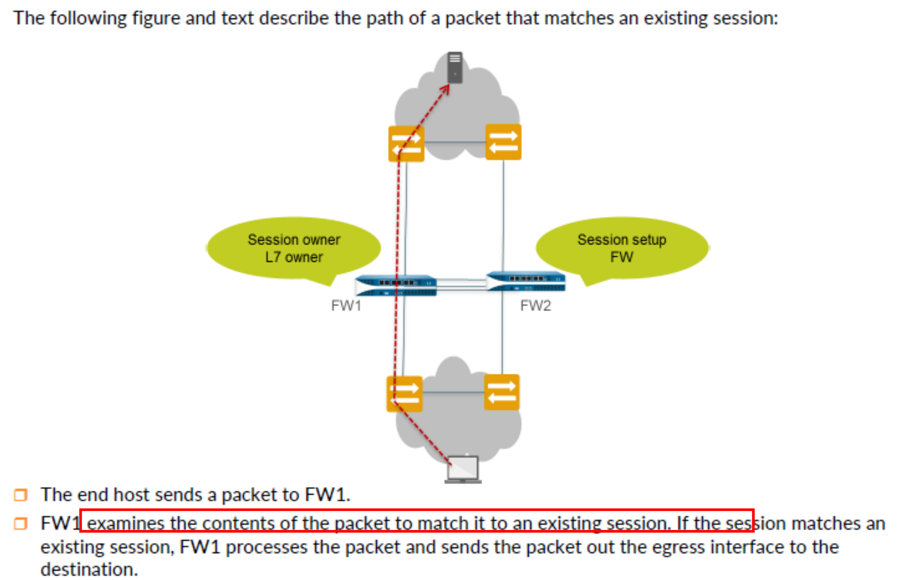
	 • Capture application packets so that you can find unique characteristics about the application on which to base your custom application signature. One way to do this is to run a protocol analyzer, such as Wireshark, on the client system to capture the packets between the client and the server. Perform different actions in the application, such as uploading and downloading, so that you will be able to locate each type of session in the resulting packet captures (PCAPs). • Because the firewall by default takes packet captures for all unknown traffic, if the firewall is between the client and the server you can view the packet capture for the unknown traffic directly from the Traffic log. • Use the packet captures to find patterns or values in the packet *contexts* that you can use to create signatures that will uniquely match the application traffic. For example, look for string patterns in HTTP response or request headers, URI paths, or hostnames. For information on the different string contexts you can use to create application signatures and where you can find the corresponding values in the packet, refer to Creating Custom Threat Signatures. **Source:** *PAN-OS Administrator's Guide, Pg. 485,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf  Dynamic Filters: A dynamic filter is a set of applications that is created based on any combination of the filter criteria: category, subcategory, behavioral characteristic, underlying technology or risk factor. Security policies (e.g. deny, allow, scan) can be applied to dynamic filters. The security policy is then enforced for application traffic that matches the filter criteria. *App-ID Tech Brief,* https://www.paloaltonetworks.com/apps/pan/public/downloadResource?pagePath=/content/pan/en_US/resources/techbriefs/app-id-tech-brief

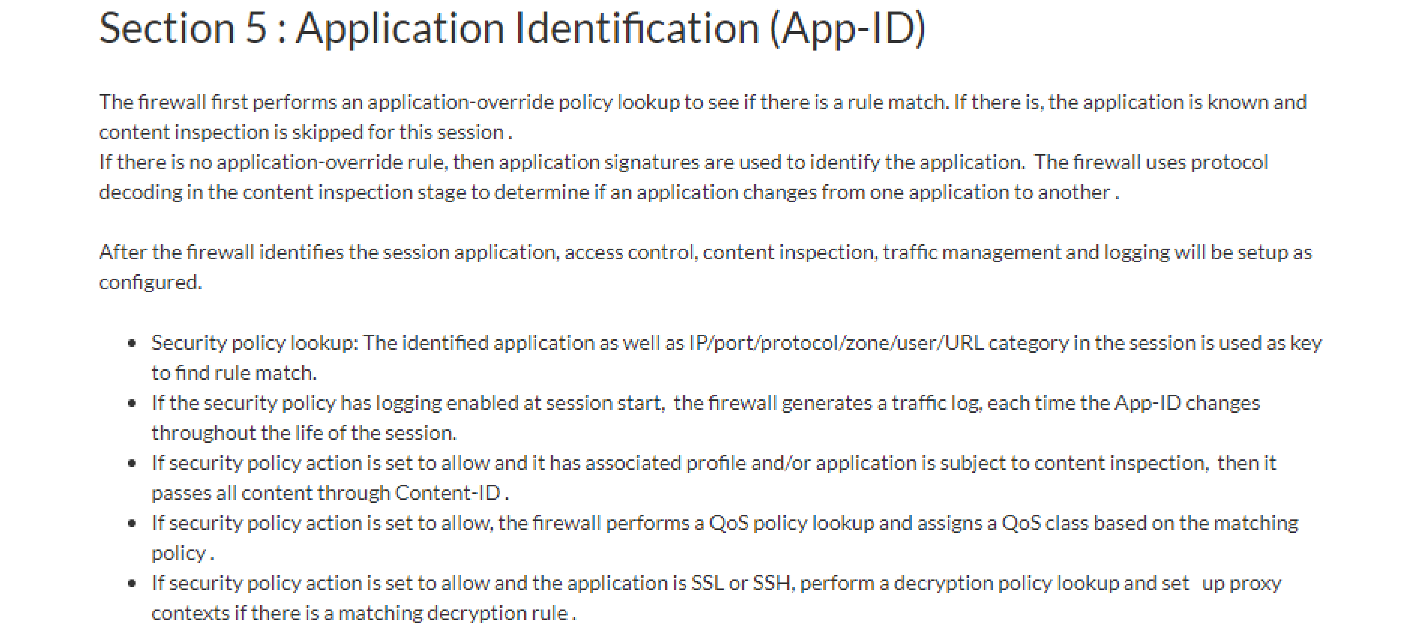
	 Create a Custom Application with a signature and attach it to a security policy, or create a custom application and define an application override policy—A custom application allows you to customize the definition of the internal application—its characteristics, category and sub-category, risk, port, timeout—and exercise granular policy control in order to minimize the range of unidentified traffic on your network. Creating a custom application also allows you to correctly identify the application in the **ACC** and traffic logs and is useful in auditing/reporting on the applications on your network. For a custom application you can specify a signature and a pattern that uniquely identifies the application and attach it to a security policy that allows or denies the application. Alternatively, if you would like the firewall to process the custom application using fast path (Layer-4 inspection instead of using App-ID for Layer-7 inspection), you can reference the custom application in an application override policy rule. An application override with a custom application will prevent the session from being processed by the App-ID engine, which is a Layer-7 inspection. Instead it forces the firewall to handle the session as a regular stateful inspection firewall at Layer-4, and thereby saves application processing time. For example, if you build a custom application that triggers on a host header *www.mywebsite.com*, the packets are first identified as *web-browsing* and then are matched as your custom application (whose parent application is web-browsing). Because the parent application is web-browsing, the custom application is inspected at Layer-7 and scanned for content and vulnerabilities. If you define an application override, the firewall stops processing at Layer-4. The custom application name is assigned to the session to help identify it in the logs, and the traffic is not scanned for threats. **Source:** *PAN-OS Administrator's Guide, Pg. 475,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 Enforce QoS Based on DSCP Classification A Differentiated Services Code Point (DSCP) is a packet header value that can be used to request (for example) high priority or best effort delivery for traffic. Session-Based DSCP Classification allows you to both honor DSCP values for incoming traffic and to mark a session with a DSCP value as session traffic exits the firewall. This enables all inbound and outbound traffic for a session can receive continuous QoS treatment as it flows through your network. For example, inbound return traffic from an external server can now be treated with the same QoS priority that the firewall initially enforced for the outbound flow based on the DSCP value the firewall detected at the beginning of the session. Network devices between the firewall and end user will also then enforce the same priority for the return traffic (and any other outbound or inbound traffic for the session). **Source:** *PAN-OS Administrator's Guide, Pg. 664,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 N FW Session Setup/Slowpath FW Fastpath Firewall session lookup Session match found? Y Forwarding lookup Get egress interface/zone and VSYS from L3 route, L2 FDB lookup, etc L2-4 Firewall processing Discard packet if session not in active state, update session lifetime, do NAT if applicable Application Identification NAT policy lookup (If destination NAT is present on matched rule, do second forwarding lookup to get final/real Egress interface/zone) SSL proxy: decrypt packet if applicable Firewall security policy lookup (Use application "ANY" to see if there is any rule match that allow packet for given addresses and ports. By default allow same zone and deny different zones if no match for configured rules) Session App identified? N Y App-override policy match? Y N Pattern-based application identification Content inspection applicable? N Y Security policy lookup based on application Rule match with action allow? N Discard packet Y Create and install session Content Inspection (SP3/CTD) Content inspection (protocol parsing/decoding, content matching, tunneled application detection) Rule match with action allow? N Y Discard packet Application changed from content inspection? Y N Content inspection setup (Setup SP3 if security profile is specified, set session to discard if security rule action deny, also set QoS class from QoS policy lookup) Detection result from inspection? N Y Application is SSL and decryption policy match? N Y Apply security-profile action (send alert, set session to discard ...) SSL proxy: re-encrypt packet if applicable SSL proxy: mark session to be proxied **Source:**https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081

	 The firewall uses the HA3 link to send packets to its peer for session setup if necessary. The following figure and text describe the path of a packet that firewall FW1 receives for a new session. The red dotted lines indicate FW1 forwarding the packet to FW2 and FW2 forwarding the packet back to FW1 over the HA3 link. Session owner performs Layer 7 processing Session setup FW HA1 HA2 HA3 FW1 FW2 □ The end host sends a packet to FW1. □ FW1 examines the contents of the packet to match it to an existing session. If there is no session match, FW1 determines that it has received the first packet for a new session and therefore becomes the session owner (assuming **Session Owner Selection** is set to **First Packet**). □ FW1 uses the configured session setup load-sharing option to identify the session setup firewall. In this example, FW2 is configured to perform session setup. □ FW1 uses the HA3 link to send the first packet to FW2. □ FW2 sets up the session and returns the packet to FW1 for Layer 7 processing, if any. □ FW1 then forwards the packet out the egress interface to the destination. **Source:** *PAN-OS Administrator's Guide, Pg. 222,* https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 The following figure and text describe the path of a packet that matches an existing session: □ The end host sends a packet to FW1. □ FW1 examines the contents of the packet to match it to an existing session. If the session matches an existing session, FW1 processes the packet and sends the packet out the egress interface to the destination. **Source:** *PAN-OS Administrator's Guide, Pg. 222*, https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/framemaker/80/pan-os/pan-os.pdf

	 Section 5 : Application Identification (App-ID) The firewall first performs an application-override policy lookup to see if there is a rule match. If there is, the application is known and content inspection is skipped for this session . If there is no application-override rule, then application signatures are used to identify the application. The firewall uses protocol decoding in the content inspection stage to determine if an application changes from one application to another . After the firewall identifies the session application, access control, content inspection, traffic management and logging will be setup as configured. • Security policy lookup: The identified application as well as IP/port/protocol/zone/user/URL category in the session is used as key to find rule match. • If the security policy has logging enabled at session start, the firewall generates a traffic log, each time the App-ID changes throughout the life of the session. • If security policy action is set to allow and it has associated profile and/or application is subject to content inspection, then it passes all content through Content-ID . • If security policy action is set to allow, the firewall performs a QoS policy lookup and assigns a QoS class based on the matching policy . • If security policy action is set to allow and the application is SSL or SSH, perform a decryption policy lookup and set up proxy contexts if there is a matching decryption rule . **Source:** https://live.paloaltonetworks.com/t5/Learning-Articles/Packet-Flow-Sequence-in-PAN-OS/ta-p/56081 Based on information identified from the packet, the Accused System and Method defines how the traffic flow will be processed. **P.R. 3-1(g)**: If a party claiming patent infringement asserts that a claim element is a software limitation, the party need not comply with P.R. 3-1 for those claim elements until 30 days after source code for each Accused Instrumentality is produced by the opposing party. Accordingly, Implicit reserves the right to amend and/or supplement its identification and evidence with respect to this element.
Claim 2	**Exemplary Evidence of Infringement**
2 The apparatus of claim 1, wherein the key value includes an IP address and one or	The Accused System and Method uses the apparatus of claim 1 and creates a key value based on an IP address and one or more TCP port addresses.